CHIP

Die großen Themen der digitalen Welt als **E-Paper** Mit 27 Seiten

Windows 10: Sicherheit & Datenschutz

Die wichtigsten Einstellungen für mehr Privatsphäre und den besten Schnüffelschutz

Plus: Nie wieder Datenverlust! Komfortable Tools für Ihre Backup-Strategie

Praxis 10

Windows 10: Sicherheit und Datenschutz

So sicher ist WINDOWS 10

Im aktuellen Windows 10 stecken viele Features, die Systemsicherheit und Datenschutz aushöhlen. Wir zeigen, worauf man achten sollte

CHIP 11/2015

Der beste Browser

Windows 10 setzt als neuen Standardbrowser auf Edge. CHIP zeigt, ob er mit Chrome, Firefox, Opera und Vivaldi mithalten kann

CHIP 11/2015

Schutz vor Viren & Co: Defender

Der Windows Defender ist fest ins Betriebssystem integriert und schützt Ihren Rechner vor Viren und Spyware – ganz ohne Ihr Zutun

CHIP Windows 10 Handbuch

Mehr Sicherheit dank Windows Firewall

Mit der ins Betriebssystem integrierten Firewall verhindern Sie Zugriffe von Apps aufs Internet und regeln Empfang und Versand von Datenpaketen

CHIP Windows 10 Handbuch

Nie wieder Datenverlust

Windows 10 bietet ein paar wichtige Tools und Funktionen, um Ihre Daten zu sichern. Wir zeigen, wie Sie diese optimal einsetzen

CHIP Windows 10 Handbuch

Benutzerkonten: Mehrere Nutzer – ein PC

Hier zeigen wir Ihnen, wie Sie neue Konten anlegen und die Zugriffsrechte Ihrer Kinder mit einem besonderen Konto beschränken können

CHIP Windows 10 Handbuch

Windows 10 ohne Datenspionage

Das neue Microsoft-System ist fast durchweg geglückt. Doch kein Windows vorher war so scharf auf Ihre Daten. Wir zeigen, wie Sie seine Neugier zähmen

CHIP Windows 10 Handbuch

In diesem E-Paper finden Sie sorgfältig ausgewählte Artikel aus dem Archiv der CHIP-Redaktion. In den Texten genannte DVDs können Sie unter chip-kiosk.de nachbestellen

11 Seiten
Windows 10
+
Browsertest

So sicher ist WINDOWS 10

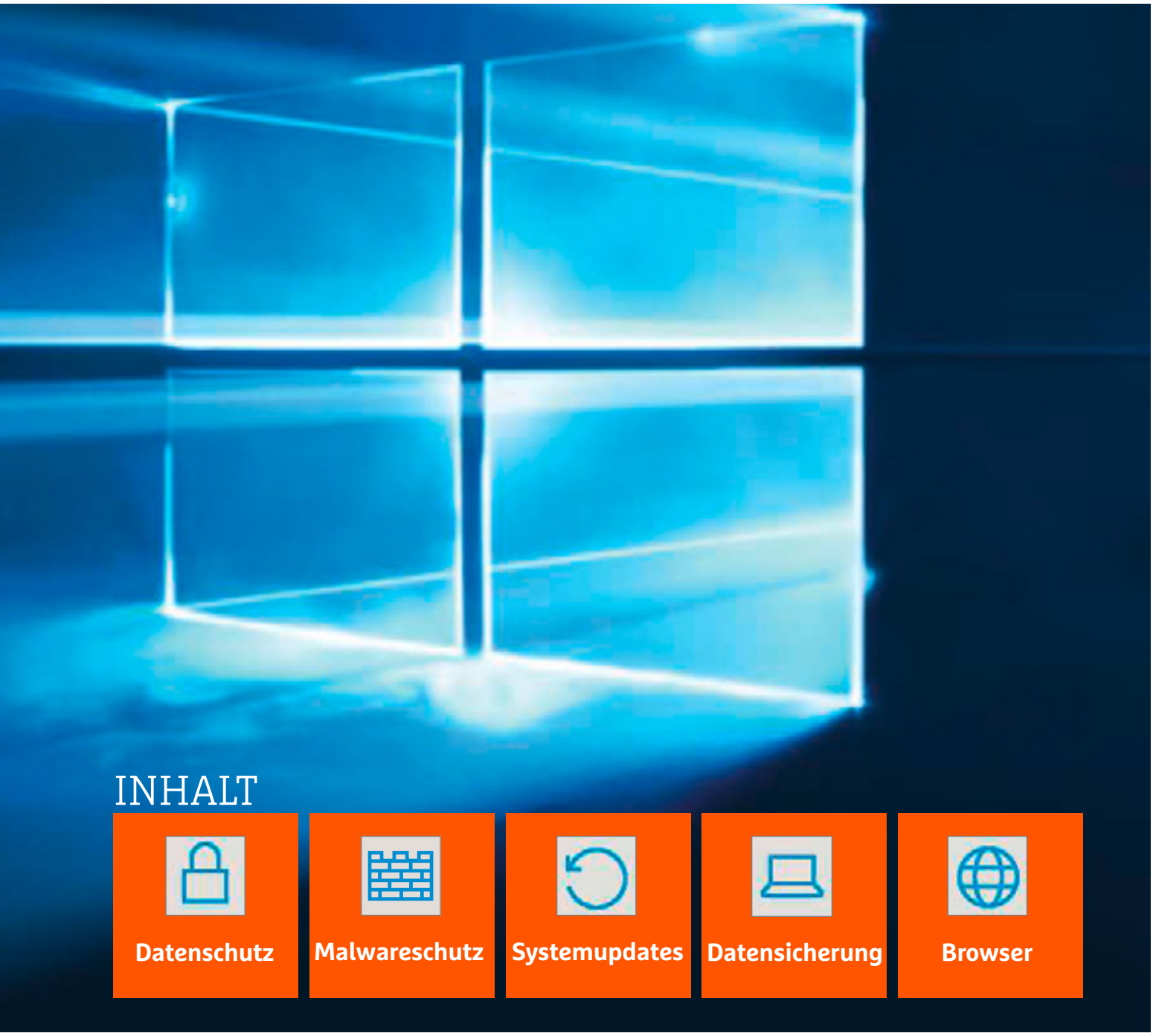
Im aktuellen Windows 10 stecken viele Features, die Systemsicherheit und Datenschutz aushöhlen. Wir zeigen, worauf man achten sollte

Von Markus Mandau

Tools auf Heft-DVD:
Kategorie Win10

Selten hat die Windows-Gemeinde eine neue Betriebssystem-Version so sehnsüchtig erwartet wie das Windows mit der Nummer 10. Schon am ersten Wochenende haben laut einer Auswertung von Statcounter drei Prozent der PC-Nutzer das neue System aufgespielt. Der Webdienst registriert die Zugriffe auf über drei Millionen Webseiten und wertet die darin enthaltenen Systemangaben aus. Mitte August waren dann schon rund zehn Prozent der Deutschen mit der Nummer 10 unterwegs. Da werden Erinnerungen wach an den Launch von Windows 7, der ähnlich schnell verlief. Wie damals von Vista wollen sich heute viele so schnell wie möglich vom ungeliebten 8.1 verabschieden. Zumal Microsoft den Versionssprung erstmals gratis anbietet, wenn man das Upgrade innerhalb des ersten Jahres aufspielt.

Wer auf sein geliebtes Windows 7 schwört, den lockt Microsoft ebenfalls mit dem Gratisangebot, doch der Sprung von 7 auf 10 ist größer, als man denkt: Windows 10 ist so stark mit internetbasierten Services verknüpft, wie man es sonst nur von mobilen Betriebssystemen kennt. Das wirkt sich auf die Sicherheit des Systems aus und ist nicht immer zum Vorteil des Anwenders. Ein Beispiel für den Wandel ist der digitale Assistent Cortana. Einmal aktiviert, analysiert er das Verhalten des Anwenders und macht darauf basierende Vorschläge, was ihn interessieren könnte. Dazu benötigt Cortana unter anderem Zugriff auf Kontakte, Browser-History, Systemsuche und Kalender. Wie Siri unter iOS funktioniert Cortana nur, wenn der Assistent das Nutzerverhalten überwacht und die Informationen in die Microsoft-Cloud schickt. Der faustische Pakt „Privatsphäre gegen



Funktionalität“ zieht sich als roter Faden durch Windows 10, und den gilt es zu aufzulösen. Am Ende sollte immer der Nutzer entscheiden, welche und wie viele Daten er preisgibt. Für Cortana gilt: Sie können den Assistenten einfach abschalten (siehe dazu CHIP 09/2015, S. 33). Andere Datenschnüffeleien des Systems lassen sich nur schwer bis gar nicht unterbinden. Wir klären auf, welche Funktionen Sie abstellen können und was Anti-Spy-Tools bringen.

Systemschnüffler und Virenwächter

Auch der altbekannte Virenschutz Defender kommt ohne eine Analyse in der Cloud nicht aus. Welche Sicherheitsfunktionen er mitbringt, erläutern wir Ihnen. Noch grundlegender hat Microsoft die Update-Funktion renoviert. Das wirkt sich langfristig auf die Stabilität des Systems aus, mit Risiken und Nebenwirkungen für den Anwender (siehe Systemupdates. Traditionell bewährt haben sich in Windows die Datensicherungsfunktionen. Ob Sie überhaupt ein separates Backup-Programm brauchen, klären wir .

Abschließend sollten Sie beim Upgrade auf Windows 10 noch eine grundlegende Entscheidung treffen: Lohnt sich der Umstieg auf Microsofts neuen Browser Edge? In einem Vergleichstest zeigen wir, ob Edge in Sachen Sicherheit, Performance und Komfort den Internet Explorer überholt und mit den User-Favoriten Firefox und Chrome auf Augenhöhe ist. Denn nirgendwo ist man als Windows-Nutzer so verwundbar wie beim Surfen im Internet – da kann das übrige Betriebssystem noch so sicher sein.

testtechnik@chip.de

Windows 10

Datenschutz maximieren

Microsoft hat Windows 10 stark mit seinen Online-Services verzahnt. Wer sich daran stört, kann das mit ein wenig Aufwand abschalten

75 Millionen Installationen nach vier Wochen demonstrieren, wie sehr die Windows-Gemeinde die Version 10 erwartet hat. Gleichzeitig erschallt der öffentliche Aufschrei wegen übermäßiger Datenschnüffelei des neuen Betriebssystems: Zwei so unterschiedliche Institutionen wie der Datenschutzbeauftragte der Schweiz und der russische Generalstaatsanwalt prüfen die Rechtmäßigkeit dieser Windows-Einstellungen in ihren jeweiligen Ländern. Auch die Passage 7b der Nutzungsbedingungen (siehe rechts) hat für Furore gesorgt. Man kann sie so verstehen, dass Microsoft das Installieren gehackter Games nachprüfen und unterbinden darf. Laut Boris Schneider-Johne, Produktmanager für Windows 10 bei Microsoft Deutschland, bezieht sich der Abschnitt nur auf die Nutzung von Xbox Live. Trotzdem haben daraufhin einige beliebte Torrent-Tracker die Nutzer von Windows 10 aus ihren Peer-to-Peer-Tauschbörsen verbannt, in der diese Games kursieren. Nur ein Fall von Paranoia?

Wenn Windows zu persönlich wird

In der Tat sendet Windows 10 eine Menge Daten an Microsoft, wenn der User bei der Einrichtung einfach den Express-Einstellungen gefolgt ist. Hat er dann noch ein Online-Profil angelegt, nutzt er den Cloudspeicher OneDrive und aktiviert Cortana, erhöht sich der Datenverkehr zu den Microsoft-Servern nochmals. Dabei muss man sich klarmachen, dass iOS und Android eine ähnlich starke Verzahnung zwischen Onlinediensten und Systemfunktionen anbieten – das ist also nichts Neues, sondern vielmehr Teil der Windows-Modernisierung. Dazu gehört auch, dass Microsoft personalisierte Werbung im Browser oder Onlinekonto einblendet (siehe rechts).

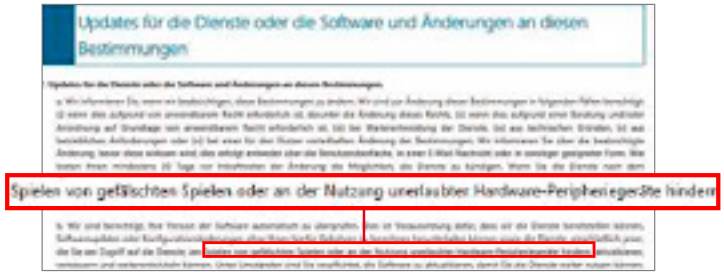
Zudem hat auch Windows 7 keine reine Weste und sendet Daten nach Hause. Das betrifft vor allem Sicherheitsfeatures wie SmartScreen und die automatisch aktivierte Teilnahme an Microsofts SpyNet. Dabei handelt es sich um eine Funktion des Malwareschutzes Defender, der verdächtige Samples in die Microsoft-Cloud schickt. Der SmartScreen überprüft Webseiten und aus dem Web geladene EXE-Dateien, um den Nutzer rechtzeitig etwa vor Phishing-Attacken zu warnen. Dazu greift die Windows-Funktion auf eine Datenbank zu, die Informationen von über 1 Milliarde Windows-Installationen enthält. Wie in Windows 7 und 8 sind beide Features auch in Windows 10 ab Werk aktiv, lassen sich aber im Nachhinein deaktivieren.

In Windows 10 genügt unter »Einstellungen | Datenschutz« ein Klick auf die »Datenschutzbestimmungen«, um zu sehen, welche Informationen Microsoft abgreift. Und das sind nicht wenige. Auch das »Datenschutz«-Menü beeindruckt durch die Anzahl der Funktionen, die sich deaktivieren lassen. Und doch findet man hier längst nicht alle Schalter, um Windows in einen „Offline-Modus“ zu versetzen. Auch das Feature Windows Customer Experience Improvement Program (CEIP) unter »Feedback und Diagnose«, übrigens auch Teil von Windows 7, sammelt und sendet Daten über laufende Software zu Microsoft – mit dem Ziel, deren Interaktion mit Windows zu optimieren. In Windows 7 und 8 lässt sich CEIP deaktivieren – über die

INFO

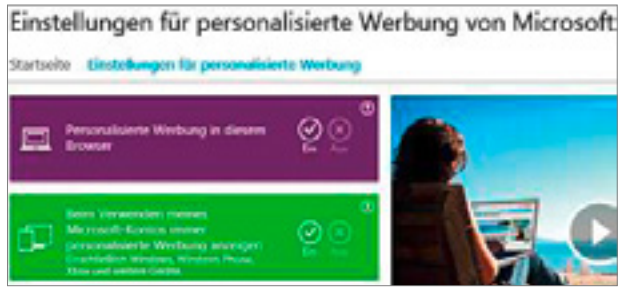
Ein Sturm im AGB-Wasserglas

Darf Windows 10 das Ausführen gehackter Spiele verhindern? Die Passage in den AGBs beziehe sich nur auf Xbox Live, sagt Microsoft.



Personalisierte Werbung ist aktiviert

Microsoft analysiert das Verhalten der Nutzer, die mit einem Online-Profil angemeldet sind, und blendet personalisierte Werbung ein. Abschalten lässt sich das in »Einstellungen | Datenschutz | Allgemein«.

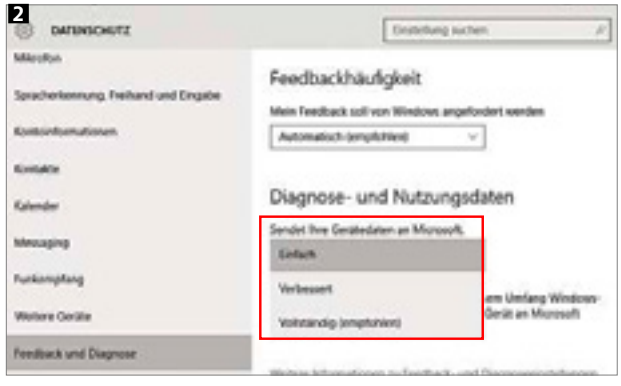


Datenschutzoptionen durchgehen

Das Gros der „Schnüffel-Funktionen“ wird im »Datenschutz«-Menü 1 deaktiviert. Dazu sind rund 30 Klicks erforderlich. Einige Funktionen wie das Senden von Diagnosedaten 2 zum Zusammenspiel von Software und OS lassen sich nicht mehr komplett abschalten.

1

2



Suchfunktion »CEIP« aufrufen und abschalten. In Windows 10 fehlt das. Hier hilft nur die viel zu komplizierte Handarbeit – neue Registry-Einträge anlegen plus laufende Systemdienste deaktivieren – oder ein Anti-Spy-Tool (siehe unten).

Manche Funktionen sehen problematisch aus, entpuppen sich bei näherem Hinsehen aber als relativ harmlos: In den »Systemeinstellungen« ermöglicht das aus Windows Phone bekannte WiFi Sense unter »Netzwerk und Sicherheit | WLAN | WLAN-Einstellungen verwalten« den Austausch von WLAN-Zugängen mit Freunden aus sozialen Netzwerken und den Kontakten. Das ist ungefährlicher, als es sich anhört, denn der Austausch gibt nicht das WLAN-Passwort weiter und die Freunde haben im Heimnetz nur Webzugriff. Leider hat man im Windows-Menü nur die Wahl, alle Facebook-Freunde sowie Skype- und Outlook-Kontakte zu aktivieren oder niemanden.

Windows telefoniert fleißig nach Hause

In einem Experiment haben wir den ausgehenden Datenstrom überprüft, den Windows zu Microsoft sendet. Das geht relativ unkompliziert, da die FritzBox via Paketmitschnitt erlaubt, den Datenverkehr abzufangen (Anleitung auf Heft-DVD). Mit dem Tool Wireshark lässt sich der Mitschnitt danach analysieren (siehe rechts). Aufgezeichnet haben wir lediglich den Windows-Start, die erste Minute im Betrieb, das Öffnen des Start-Menüs mit den Live-Kacheln sowie einen Klick in die Windows-Suche. Bei aktiviertem Online-Profil und mit den Windows-Einstellungen out of the box gingen in der Zeit rund 200 Verbindungen an Microsoft-Services hinaus, darunter Update-Server, Live-Login, SpyNet, OneDrive und Bing. Beim zweiten Versuch haben wir die »Datenschutz«-Einstellungen aktiviert, Cortana abgestellt und ein Offline-Profil angelegt. Dabei hat sich die Anzahl der Verbindungen auf etwa 100 halbiert. Kontaktiert hat Windows dabei unnötigerweise den Live-Login trotz Offline-Profil. Es reicht also nicht aus, nur die vom System angebotenen Services zu deaktivieren. Microsoft sagt dazu, dass Windows 10 die Verbindungen aufbaut, um Updates und neue Funktionen einzuspielen.

Im Zuge der Schnüffelaffäre wurde eine Reihe von Anti-Spy-Freeware für Windows 10 veröffentlicht. Die Tools bieten Zugriff auf Sendefunktionen, die man im System nicht ohne Weiteres abschalten kann. Wir haben O&O ShutUp10 (auf Heft-DVD) ausgewählt und dort alles aktiviert – auch Optionen, die das Tool nicht empfiehlt. Zusätzlich haben wir alle Microsoft-Apps deinstalliert, die mit dem System ausgeliefert werden. Dadurch konnten wir die Anzahl der Verbindungen auf acht reduzieren (siehe rechts), mussten in diesem Zuge aber auch sinnvolle Services wie Defender und SmartScreen abschalten. Ob und in welchem Umfang man ein Anti-Spy-Tool einsetzt, muss am Ende jeder für sich entscheiden. Zu empfehlen sind vor allem Programme, die auch alle Einstellungen wieder rückgängig machen. Zudem sollte man vorher eine Systemsicherung anlegen, falls etwas schiefgeht. Und nicht jedes Tool ist unproblematisch. So schlägt zum Beispiel DoNotSpy10 bei der Installation auch die Adware OpenCandy vor. Da gilt es aufzupassen und dieses Häkchen zu entfernen, sonst spielt die Anti-Spyware ihre eigene Spyware auf.

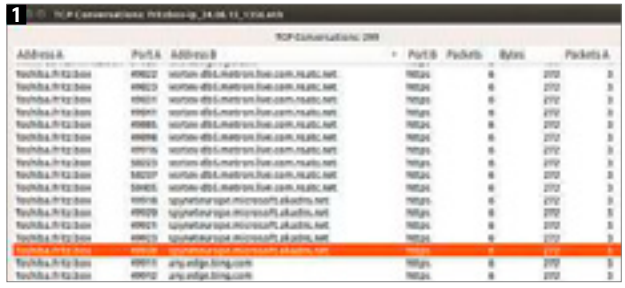
Insgesamt ist Windows 10 das Kind einer Zeit, in der digitale Assistenten das Nutzerverhalten überwachen und analysieren. Gut ist, dass Microsoft offen damit umgeht und in den Datenschutzbestimmungen aufzählt, welche persönlichen Informationen das System erfasst. Trotzdem hätte Microsoft es den Nutzern einfacher machen können. Momentan stehen noch ein paar Dutzend Klicks an, ehe man sich seiner Privatsphäre so sicher sein kann wie in Windows 7. Ein Schalter für einen Privat-Modus, wie ihn die Anti-Spy-Tools im Prinzip bieten, hätte Windows 10 gut zu Gesicht gestanden. →

INFO

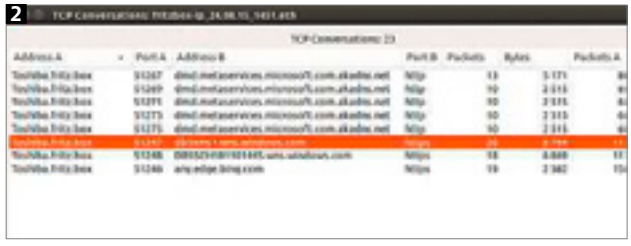
So viele Verbindungen baut Windows 10 auf

Über eine FritzBox-Funktion kann man den Datenverkehr mitschneiden. Out-of-the-Box baut Windows 10 in der ersten Minute rund 200 TCP-Verbindungen **1** auf. Schaltet man möglichst viele ab und nimmt ein Anti-Spy-Tool, lässt sich der Datenverkehr stark reduzieren **2**.

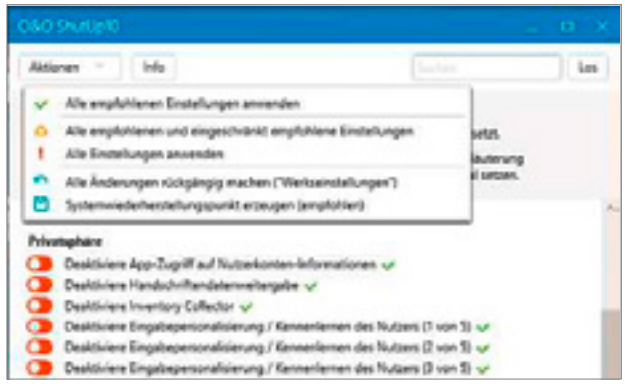
1



2



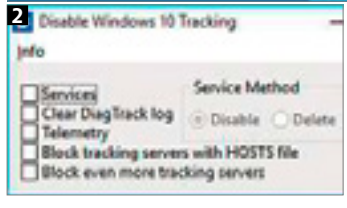
Diese Tools bringen Windows zum Schweigen



Ein gutes Beispiel für ein Anti-Spy-Tool ist O&O ShutUp10: Es empfiehlt sinnvolle Maßnahmen und macht Änderungen rückgängig

1

2



Einige Anti-Spy-Tools sind so neu, dass Windows 10 eine Warnung ausgibt **1**. Das gilt auch für das einfach gestrickte Open-Source-Tool Disable Windows 10 Tracking **2**.

+ **Microsoft versteckt die Datensammelei in Windows 10 nicht und bietet Systemfunktionen, um zumindest einige Services abzustellen.**

– **Nicht alle Online-Services respektieren die Privatsphäre. Aktuell kann man sie nur über ein Anti-Spy-Tool wiederherstellen.**

Windows 10

Schutz vor Malware

Früher oder später wird Windows 10 das Hauptziel von Malware-Attacken. Am integrierten Virenschutz hat sich leider wenig getan

Das Dilemma ist bekannt: Die systemeigenen Security Essentials in Windows 7 oder der Defender in 8 landen bei Tests von Security-Suiten für gewöhnlich auf dem letzten Platz. Laut Andreas Marx, Geschäftsführer des führenden deutschen Antiviren-Labors AV-Test, wird das mit Windows 10 nicht besser: „Wir haben in den letzten Wochen bereits einige Tests durchgeführt, um festzustellen, ob die Schutzwirkung des Defenders in Windows 10 optimiert wurde. Doch die Leistung bleibt die gleiche, es gibt keine messbaren Unterschiede." Von einer dreistelligen Anzahl an bösartigen Samples hat der Defender etwa 90 Prozent geblockt. Dabei handelt es sich um Zero-Day-Angriffe, also bisher nicht bekannte Malware, inklusive bösartiger Webseiten und verseuchter E-Mails. „Das Ergebnis", urteilt Marx, „liegt deutlich unter dem Branchendurchschnitt."

Security-Suiten durchweg kompatibel

AV-Test hat auch alle üblichen Antiviren-Lösungen für Privatanwender unter Windows 10 ausprobiert. Das Fazit: Die Kernfunktionen laufen einwandfrei, sofern man bei den Updates auf dem neuesten Stand ist. „Aber ein Installationstest kann kaum klären, wie gut die Software arbeitet", so Marx. „Das wird erst ein Langzeittest aufzeigen." Nicht wenige Hersteller von Schutzprogrammen äußern sich zum Thema Kompatibilität zurückhaltend. Sie beklagen die kurze Vorlaufzeit von der Freigabe bis zur Veröffentlichung von Windows 10. Einige Änderungen an den Schnittstellen machen ihnen ebenfalls zu schaffen. Auch der neue Edge-Browser ist eine harte Nuss: Da er noch keine Plug-ins zulässt, kann man ihn besonders bei verschlüsselten HTTPS-Verbindungen nur schwer überwachen. Hier gibt Marx aber Entwarnung: „Die von uns regelmäßig geprüften Schutzprogramme erkennen Schädlinge beim Einsatz von Edge so gut wie unter anderen Browsern in Windows 7 oder 8."

Eine der neuen Schnittstellen in Windows 10 ist das Anti-Malware Scan Interface (AMSI). Über AMSI kann jedes Programm verdächtigen Code, den es aus dem Web erhält und in seinem Arbeitsspeicher-Bereich vorfindet, an den Malware-Scanner schicken (siehe rechts). Hat der User keine externe Schutzlösung installiert, springt der Defender ein. AMSI hilft dabei, bösartige Skripte zu entdecken, für die noch keine Signatur vorliegt, denn Virenwächter haben Probleme, gepackte oder verschlüsselte Malware-Skripte schon beim Download aus dem Web zu entdecken. Deren Bösartigkeit offenbart sich erst, wenn sie ausgepackt und ins RAM geladen werden.

Malware benötigt Sicherheitslücken, um die Schutzmaßnahmen von Windows auszuhebeln. Hier hat Microsoft nachgebessert und sein Bug-Bounty-Programm zeitgleich mit der Veröffentlichung von Windows 10 aufgestockt: Hacker oder Sicherheitsforscher, die eine Lücke entdecken und exklusiv an Microsoft senden, erhalten bis zu doppelt so hohe Prämien. Ob und wie viel diese Maßnahme bringt, lässt sich noch nicht beantworten, aber man kann hoffen, dass nun mehr Lücken vorab an Microsoft übermittelt werden.

INFO

Windows Defender mit Defiziten

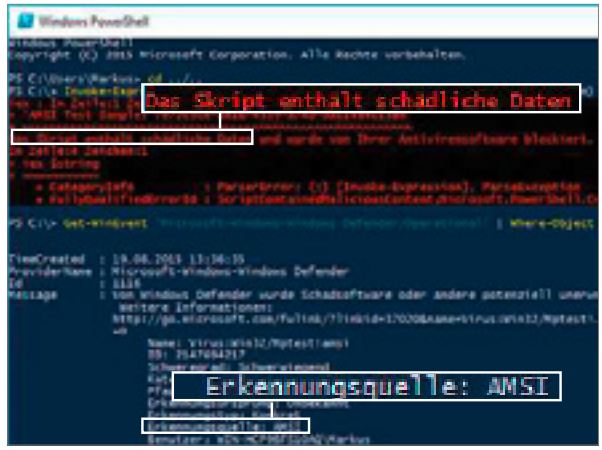
Der von Microsoft mitgelieferte Malware-Wächter Defender ähnelt nicht nur äußerlich der Version, die in Windows 8 steckt. Erste Tests zeigen, dass auch die Erkennungsrate nicht besser geworden ist.

ERKENNUNGSRATE BEI ZERO-DAY-MALWARE IN WINDOWS 10

QUELLE: AV-TEST

AMSI: Ein neues Werkzeug gegen Viren

Neu in Windows 10 ist das Anti Malware Scan Interface (AMSI). Darüber können Windows-Programme im Hintergrund den installierten Virenscanner beauftragen, verdächtigen Skript-Code zu überprüfen.



Viel Geld für neue Sicherheitslücken

Im Rahmen von Windows 10 hat Microsoft sein Bug-Bounty-Programm aufgestockt: Hacker bekommen doppelt so viel Geld, wenn sie Windows-Lücken vorab an Microsoft melden.

	Microsoft	Mozilla	Google	Yahoo	Facebook
Programmname	Bounty	Client Bug Bounty	Vulnerability Reward	Bug Bounty	whitehat
Minimum-Bounty	500 US-$	500 US-$	100 US-$	50 US-$	500 US-$
Maximum-Bounty	100.000 US-$	über 10.000 US-$	20.000 US-$	15.000 US-$	keine Höchstgrenze

+ Alte Security-Suiten laufen prinzipiell auch unter Windows 10. Eine neue Schnittstelle verbessert die Malware-Erkennung.

− Der integrierte Virenwächter Defender hat auch in Windows 10 eine schlechtere Erkennungsrate als die Konkurrenz.

Automatische Updates

Zwangs-Updates halten Windows 10 immer auf dem neuesten Stand. Das heißt aber auch: Bei Update-Fehlern steht der Anwender im Regen

Windows 10 verteilt System-Aktualisierungen und Funktions-Updates sofort und nicht nur am Patchday. Zudem verzichtet die runderneuerte Update-Funktion auf die Zweiteilung in Sicherheits-Patches und optionale Updates. Optional ist ab jetzt nichts mehr, in den »Einstellungen« über »Updates und Sicherheit« lässt sich der Updatezwang nicht ausschalten. Der Anwender hat hier die Wahl, ob das System sie automatisch im Hintergrund durchführt oder ob es ihn benachrichtigt, wenn ein Neustart erforderlich ist. Im Prinzip ergibt das Sinn, denn neue Updates werden umgehend auf allen Rechnern eingespielt. Doch in der Praxis haben schon viele Anwender schlechte Erfahrungen mit der Update-Funktion gemacht.

Erst im letzten Jahr hat Microsoft eine Reihe fehlerhafter Patches ausgeliefert, die nicht wenige PCs in eine Endlos-Bootschleife schickten, welche die User über den abgesicherten Windows-Start reparieren mussten. Die Fehlerflut ebbte 2015 zwar etwas ab, doch noch im Mai haben zwei fehlerhafte Treiber-Patches zur Darstellung von Schriften Windows 7 in die Knie gezwungen. Mit Windows 10 geht man eine Wette auf die Zukunft ein, dass Microsoft solche Probleme in den Griff bekommt. Genau genommen gehen diejenigen die Wette ein, die Windows 10 Home installiert haben – das Gros der Privatrechner. In der Home-Version lässt sich nur der Zwang zur automatischen Treiber-Aktualisierung in der Systemsteuerung ausschalten, eine Option, die schon Windows 7 hatte. Die weniger verbreitete Pro-Version erlaubt das Aufschieben von Funktions-Updates um vier Monate (siehe rechts) – Sicherheitspatches werden wie üblich sofort eingespielt. In Firmen installierte Versionen können den Zeitraum auf zwölf Monate strecken. Ob Pro-Nutzer davon Gebrauch machen sollten, ist fraglich, denn damit verzichten sie auch auf sinnvolle Windows-Neuerungen. Anti-Spy-Tools bieten darüber hinaus an, die Update-Funktion komplett auszuschalten. Gleichzeitig warnen sie vor der Deaktivierung, da sie auch Sicherheitspatches blockt.

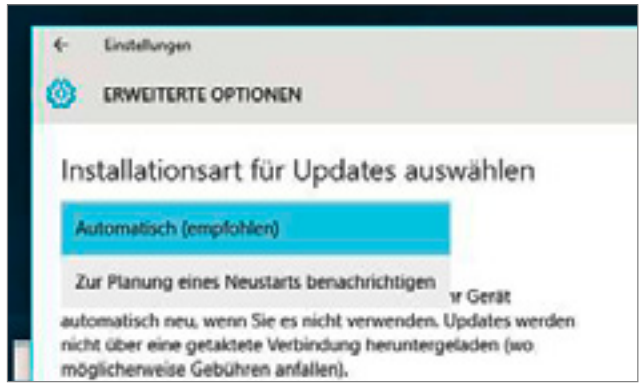
Anwender müssen Microsoft vertrauen

In den »erweiterten Optionen« des Update-Menüs hat Microsoft unter »Übermittlung von Updates auswählen« eine weitere Neuerung versteckt. Standardmäßig ist aktiviert, dass Windows 10 Updates nicht nur von Microsoft-Servern, sondern auch von anderen Rechnern bekommt, die im Internet hängen – ein einziges großes Peer-to-Peer-Netz also, das Updates verteilt. Das ist ebenso eine Wette auf die Zukunft, denn eine Sicherheitslücke hier kann großen Schaden anrichten. Wer dem Szenario aus dem Weg gehen will, sollte die Funktion deaktivieren. Im Zusammenhang mit der neuen Update-Politik wurde Microsoft auch dafür kritisiert, dass es kaum noch Informationen herausgibt, welche Fehler die Patches beheben. Microsoft hat reagiert: Selbst Home-User können Details einsehen, zum Beispiel für welche Module ein Update aufgespielt wird. In Kürze werden auch die Zwangs-Updates der installierten Microsoft-Apps über den Store-Account abschaltbar sein. An Microsofts unerschütterlicher Haltung zu Zwangs-Updates ändert das aber nichts. →

INFO

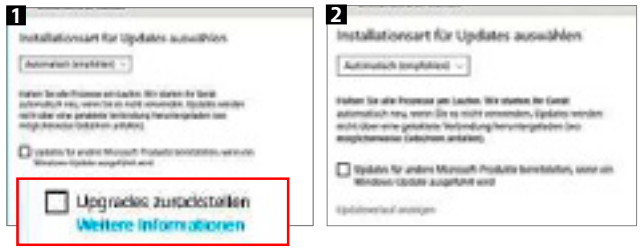
Der Patchzwang ist eingebaut

Windows 10 spielt Updates immer automatisch ein. Der Anwender kann nur entscheiden, ob er dabei selber einen Neustart durchführt.



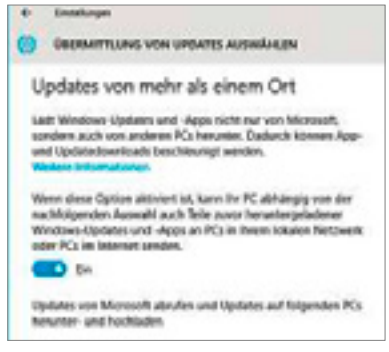
Nur die Pro-Version kann Updates verzögern

Die Update-Automatik greift in der Pro-Version nicht sofort. Der Anwender kann Windows-Updates bis zu vier Monate zurückstellen **1**. In der Home-Version fehlt dagegen diese Wahlmöglichkeit **2**.



Windows-Updates per Tool abschalten

Anti-Spy-Tools wie Win10Privacy deaktivieren auch die Update-Funktion. Als Ausweg aus dem Update-Zwang ist das nicht zu empfehlen.



Updates übers Peer-to-Peer-Netz

Ab Werk aktiv ist die Verteilung der Updates über ein Peer-to-Peer-Netz, das Windows-10-Rechner verbindet. Dieses potenzielle Sicherheitsrisiko sollte man deaktivieren.

Alle verfügbaren Windows-Updates werden sofort eingespielt und schließen bekannt gewordene Sicherheitslücken automatisch.	**Nicht wenige Updates haben sich als fehleranfällig erwiesen. In Windows 10 muss der User hoffen, dass sich das ändert.**

Windows 10

System und Daten sichern

Mit jeder neuen Version vermehrt Microsoft die Anzahl der Sicherungsfunktionen. Da fällt es schwer, den Überblick zu behalten

Seit der Version 7 bringt Windows eine Reihe von Datensicherungs-Optionen mit, die ziemlich viel von dem abdecken, was der normale Anwender so braucht. In Windows 8 kam die Cloud-Anbindung mit OneDrive hinzu. Wer das Upgrade von einer älteren Version auf Windows 10 durchführt, hat zudem in den ersten vier Wochen die Chance, auf die ältere Version zurückzugehen. Vor allem Umsteiger von Windows 7 haben jetzt mehr Möglichkeiten, was die Systemsicherung oder -reparatur angeht: Schon seit Windows 8.1 kann man das Betriebssystem per Knopfdruck auf den Auslieferungszustand zurücksetzen. Diese Aktion entspricht dem Aufspielen eines neuen Windows, wobei Windows 10 Ihnen die Wahl lässt, ob Sie Ihre persönlichen Dateien beibehalten oder löschen wollen.

Beim Auffrischen des Systems bleiben diese Daten automatisch intakt, die installierten Programme werden aber gelöscht. Hier setzt Windows von einem Installationsmedium aus die Systemdateien in den Originalzustand zurück. Unter »Systemsteuerung | Wiederherstellung« kann man dazu ein »Wiederherstellungslaufwerk erstellen«. Diese Funktion sollte eigentlich den aus Windows 7 bekannten Systemreparatur-Datenträger ersetzen. Verwirrenderweise gibt es den nach wie vor in der Systemsteuerung unter »Sichern und Wiederherstellen (Windows 7)«. Wegen der vielen Umsteiger von Windows 7 hat Microsoft diese Funktion in Windows 10 implementiert, so können Anwender alte System- und Dateisicherungen importieren.

Sicherungs-Features im System verstreut

Windows 10 hat immer noch eine Systemwiederherstellung, und die Option, Schattenkopien von Files über das Dateisystem vorzuhalten, fehlt auch nicht. Für das Backup einzelner Ordner geht man in den »Einstellungen« über den von Windows 8 bekannten »Dateiversionsverlauf«. Er verlangt ein Sicherungsmedium wie etwa eine USB-Festplatte. Diese Funktion sichert in festgelegten Intervallen automatisch Standard-Ordner wie Dokumente, Bilder und Musik. Ist man zudem mit einem Online-Profil angemeldet, aktiviert sich OneDrive und synchronisiert die Inhalte der OneDrive-Ordner, von denen man weitere im Explorer anlegen kann. Will man die Funktion konfigurieren, geht das über das OneDrive-Symbol in der Taskleiste und per Rechtsklick auf einen OneDrive-Ordner im Explorer.

Wenn es einen Kritikpunkt zum Thema Datensicherung gibt, dann die Bedienbarkeit. Windows 10 vereint viele Optionen, die Microsoft seit XP integriert hat. Dementsprechend stecken sie nicht an einem Ort, sondern sind über das System verstreut. Zusätzlich hat Microsoft auch Sicherungsfunktionen von Windows 7 in der Systemsteuerung belassen. Darunter leiden der Überblick und die Benutzerfreundlichkeit – die zentralen Faktoren beim Thema Backup. Erfahrungsgemäß betreiben Anwender eher eine systematische Datensicherung, wenn ihnen keine Hürden in den Weg gelegt werden. Diese Hürden baut Windows 10 künstlich auf. Stattdessen gehören alle Sicherungsoptionen in die »Einstellungen« des Startmenüs. Aktuell findet man dort aber nur einen Bruchteil. →

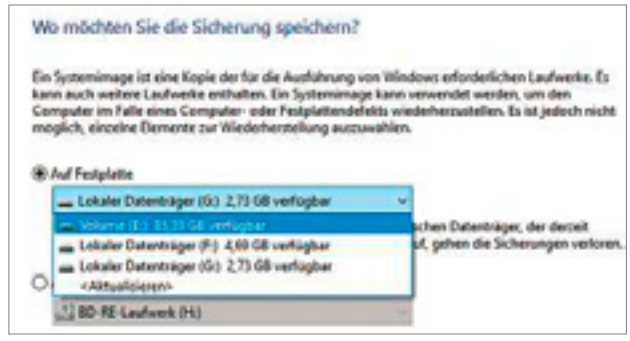
INFO

Windows-Downgrade mit eingebautem Timer

Upgrader haben vier Wochen Zeit, um zu ihrem alten System zurückzukehren. Danach bleibt ihnen nur noch, den PC zurückzusetzen, was den Ausgangszustand von Windows 10 wiederherstellt.

Systemsicherung wie unter Windows 7

Die Systemsicherung steckt immer noch in der alten »Systemsteuerung« und nicht in den neuen »Einstellungen«. Zum Erzeugen eines Systemabbilds nutzt man dasselbe Modul wie unter Windows 7.



Dateisicherung einstellen

Einzelne Ordner sichert Windows 10 im »Dateiversionsverlauf«. Die Standard-Verzeichnisse für Dokumente oder Musik sind voreingestellt. Weitere Ordner lassen sich manuell hinzufügen.

Cloud-Backup

Über das OneDrive-Symbol in der Taskleiste kann man definieren, welche Ordner mit dem Online-Speicher synchronisiert werden.

Ob das ganze Betriebssystem oder einzelne Ordner – es gibt wenig Backup-Vorhaben, die man in Windows nicht durchführen kann.

Alle Sicherungsfunktionen sind wie ein Sammelsurium über das System verstreut. Diesen Missstand beseitigt Windows 10 nicht.

Der beste Browser

Windows 10 setzt als neuen Standardbrowser auf Edge. CHIP zeigt, ob er mit Chrome, Firefox, Opera und Vivaldi mithalten kann

Von Jörg Geiger

Der beliebteste Browser der Welt wird sterben. Microsoft versetzt mit Windows 10 den Internet Explorer in den Vorruhestand. Er ist zwar noch an Bord, aber nur noch als Notnagel, um etwa Webseiten anzuzeigen, die ActiveX nutzen, oder um speziell in Unternehmen entwickelte Dienste am Laufen zu halten. Der neue Standardbrowser unter Windows 10 heißt Microsoft Edge. Er orientiert sich am minimalistischen Auftreten von Google Chrome und bringt die neue Rendering-Engine EdgeHTML mit. Wer keinen anderen Browser nachinstalliert, ist unter Windows 10 – und nur dort – automatisch mit Edge im Netz. Doch der neue Browser wird von den Usern nur zögerlich angenommen: Einen Monat nach dem Start war Windows 10 weltweit auf rund 75 Millionen Geräten installiert. Glaubt man den Zahlen von Browserstatistiken, dann gehen nicht einmal die Hälfte der Nutzer von Windows-10-Rechnern mit Edge ins Web. Wir haben getestet, was der IE-Nachfolger kann, und den neuen Browser mit Chrome, Firefox, Internet Explorer, Opera und Vivaldi verglichen.

Aktuelle Technik liegt vorne

Unser Testergebnis zeigt es klar: Mit alter Technik kann man nichts mehr gewinnen. Der betagte Internet Explorer landet auf dem letzten Platz. Er ist langsam, schlecht ausgestattet und kompliziert zu bedienen. Dabei kommt er mit der Gesamtnote befriedigend noch ganz gut weg. Doch die anderen sind einfach besser, und das geht vor allem auf das Konto aktuellerer Technik. Bis auf den Internet Explorer sind alle Kandidaten entweder komplett neu aufgebaut (Chrome, Edge), gerade im Neuaufbau begriffen (Firefox) oder verwenden den Chrome-Unterbau Chromium (Opera, Vivaldi). Im Test liegen die drei Browser mit ähnlicher Technik, nämlich Chrome sowie Opera und der noch nicht ganz fertige Vivaldi ganz vorne. Alle drei nutzen die gleiche HTML-Rendering-Engine (Blink) sowie die gleiche JavaScript-Umgebung (V8). Doch es gibt auch bei identischen Engines noch Spielraum, wie unsere Benchmarks zeigen. Vor allem im Tempo abgeschlagen folgen Firefox und Microsoft Edge. Ersterer liegt nur wegen der besseren Bedienung und Ausstattung vor Edge, der technisch die Nase vorn hat. Mozilla sollte sich mit der Renovierung beeilen, sonst verliert das Füchslein den Anschluss.

Nur Firefox und Opera bedienen Windows-Nutzer noch nicht mit einer eigenen 64-Bit-Version, alle anderen Kandidaten stehen als angepasste 32- und 64-Bit-Varianten zur Verfügung. Die beiden Microsoft-Browser konzentrieren sich nur auf Windows, Edge sogar nur auf Windows 10. Die anderen Testkandidaten bedienen neben Windows noch Linux und OS X. Dass Firefox technisch hinterherhinkt, zeigt ein kleines Detail: Nur bei Mozilla werden alle offenen Webseiten in einem Prozess gerendert. So ist das Risiko hoch, dass eine abgestürzte Webseite den ganzen Browser blockiert. Alle anderen Testkandidaten setzen dagegen auf Multiprozess-Umgebungen, packen also jedes Tab in einen eigenen Prozess. Das bringt mehr Stabilität und ist für ein flexibleres Speichermanagement von Vorteil.

JavaScript-Sieger Edge

Dies ist umso bedeutender, als Browser zu den Programmen gehören, die meist die ganze Zeit geöffnet sind und auch am meisten genutzt werden. Deshalb ist die schnelle Arbeitsgeschwindigkeit eine der wichtigsten Eigenschaften. Erste große Überraschung in unseren umfangreichen Speed-Tests war, dass Microsoft Edge alle anderen Browser bei den JavaScript-Benchmarks schlägt, sogar Testsieger Chrome. Kurios: Edge setzte sogar im Octane-Benchmark, der von

Google selbst stammt, mit 24.074 Punkten den Bestwert mit rund 1.300 Zählern mehr als Chrome. Wie sehr das die Google-Entwickler stört, zeigen die neuen Funktionen der nächsten Chrome-Version, die mit Erscheinen dieser Ausgabe zu haben sein wird. Deren Schwerpunkt ist die Beschleunigung von JavaScript-Code. Doch in der getesteten Version besetzt der Google-Browser nur Platz 2 in dieser Leistungswertung, knapp vor Opera und Vivaldi. Firefox kommt gerade mal auf 17.791 Punkte und Schlusslicht ist der Internet Explorer. Einschränkend muss man erwähnen, dass die getestete Edge-Version als einziger Browser Probleme mit dem Jetstream-Benchmark hatte, der ebenfalls die JavaScript-Leistung misst. Dazu passt, dass Edge vereinzelt an der Darstellung komplexer Seiten scheitert.

JavaScript-Verarbeitung ist zwar wichtig, aber nicht alles. Deshalb messen wir in einem umfangreichen Benchmark die Geschwindigkeit bei typischen Webaufgaben, von der Anpassung einzelner Grafiken über das Beantworten von Requests bis zur 3D-Performance. Hier rückt Chrome die Browserwelt wieder zurecht und lässt alle hinter sich, nur Vivaldi und Opera mit dem gleichen Unterbau sind auf Augenhöhe. Aber nicht nur die Browser selbst sollten schnell sein, auch der Umgang mit ihnen soll flott von der Hand gehen.

Bedienung ist Firefox-Sache

In der Tat sind alle Browser im Test einfach gehalten, lange Einarbeitungszeit ist nirgends nötig. URL oder Suchbegriff eintippen und los geht's. Manchmal steckt der Teufel bei der Bedienung aber im Detail, und Firefox hat dafür die besten Lösungen parat. Das fängt schon beim ersten Start an: Chrome und Edge zeigen sich extrem abgespeckt und blenden lediglich die URL-Zeile ein. Bei Vivaldi und Opera wird man mit den Speed-Dials begrüßt. Eigentlich keine schlechte Idee, denn dort sind die am häufigsten besuchten Webseiten zu finden. Fängt man aber gerade erst an, den Browser zu nutzen, sitzen dort beliebige Seiten. Firefox bietet neben Suche und URL-Leiste auch schnellen Zugriff auf die Einstellungen sowie Synchronisation, Verlauf und Downloads. Hier sollten sich auch Einsteiger sofort zurechtfinden. Die Neuer-Tab-Seite von Firefox, welche neue Webseiten auf Basis des bisherigen Verlaufs vorschlägt, sehen wir kritisch. Ganz Firefox-typisch lässt sich diese Tracking-Funktion aber sehr einfach und direkt auf der Neuer-Tab-Seite abklemmen.

Bei den Einstellungsmenüs liegen Firefox und Vivaldi mit klarer Gliederung und schöner Gestaltung vorne. Vivaldi bringt sogar noch eine leistungsfähige Suche mit, die uns im Firefox fehlt. Chrome klatscht die Einstellungen nur lieblos untereinander, bei Opera ist das Einstellungsmenü fast überflüssig, denn viele Optionen sind ins Opera-Menü links oben im Fenster ausgelagert. Das wirkt insgesamt unübersichtlich. Microsoft Edge geht einen neuen Weg bei den Einstellungen und setzt sie in eine Seitenleiste, die für Touchbedienung optimiert ist. Edge verhält sich damit wie eine App, was auf dem Desktop unnötig gedrängt wirkt. Da Edge aber ohnehin der Browser mit den wenigsten Einstellungen im Test ist, geht das knappe Menü in Ordnung. Der Internet Explorer mit seinen verschachtelten Einstellungsfenstern, Menüs und Untermenüs wirkt gegenüber dem restlichen Testfeld wie aus einer anderen Welt.

Ausstattung nicht überall satt

An anderer Stelle ist ein bisschen mehr durchaus wünschenwert: Profis werden von Chrome und Firefox am besten bedient, denn diese beiden Browser haben neben den finalen Versionen, die hier getestet wurden, auch Betas und Entwicklervarianten am Start. Wer also die Funktionen von morgen schon heute ausprobieren will, kann das bei Chrome und Firefox sehr einfach machen und in den →

AUS DEM TESTLABOR

Chrome hängt die anderen ab

Browser sollten nicht nur bei einer Spezialaufgabe schnell sein, sie müssen typische Webaufgaben von Anfang bis Ende zügig erledigen. Genau das messen wir im Browsermark nach.

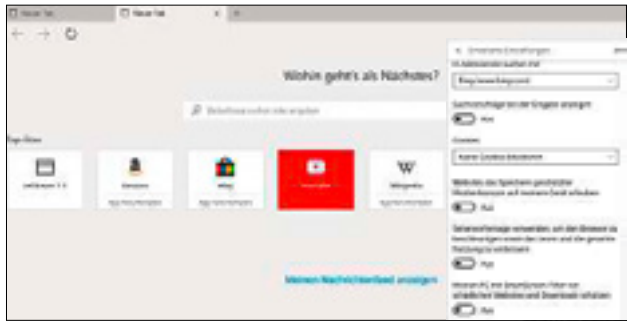
BROWSERMARK (ALLROUND SPEED-TEST) (ANGABEN IN PUNKTEN)

Firefox ist am einfachsten

Bei der Bedienung liegt Firefox vorne. Kein Browser nimmt seine User so gut an die Hand und zeigt so übersichtliche Einstellungen.

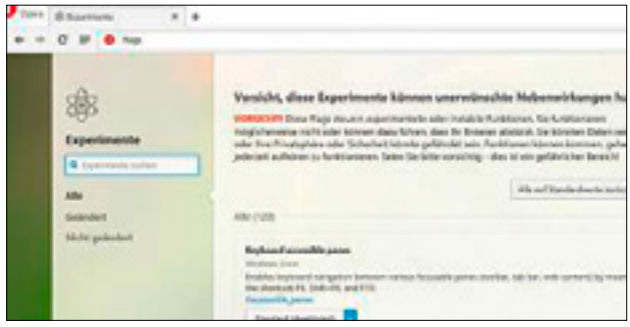
Als App konzipiert

Microsoft Edge ist auch auf dem Desktop eine App. Das sieht man zum Beispiel am gestauchten Einstellungsmenü an der Seite.



Versteckte Profifunktionen

Opera lädt unter »about:flags« zwar auch zu Experimenten ein, aber Chrome und Firefox bieten Bastlern die größeren Spielwiesen.



Windows 10

Entwicklerkanal wechseln. Ohnehin führen die beiden Browser ein Kopf-an-Kopf-Rennen um die meisten Features und bringen alle sechs Wochen neue Versionen auf den Markt. Auch in den offiziellen Versionen haben Firefox und Chrome viele versteckte Profifunktionen parat: Firefox zum Beispiel bündelt diese Einstellungen unter »about:config«, Chrome hinter »about:flags«. Auch Opera und Vivaldi kennen die große Flag-Spielwiese, dagegen sind die experimentellen Features von Microsoft Edge sehr überschaubar und vor allem noch nicht sonderlich eindrucksvoll.

Doch wir haben nicht nur Profifunktionen bewertet, im Alltag kommt es auf Brot-und-Butter-Features an. Viele User rüsten ihren Browser gerne mit Diensten nach, sei es mit einem Werbeblocker, einem VPN-Plug-in oder speziellen Downloadern für ihre Lieblingsseiten. Hier liefern sich wieder Chrome und Firefox einen knappen Showdown. Der Fuchs ist immer noch der König der Erweiterungen, obwohl es auch für Chrome jede Menge Extensions gibt. Die anderen Browser haben das Nachsehen.

An Chrome gefällt, dass er nicht nur einen PDF-Viewer, sondern als einziger Kandidat auch ein Flash-Plug-in mitliefert und dieses regelmäßig automatisch aktualisiert. Ähnlich komfortabel sind die Microsoft-Browser, die dafür allerdings das in Windows integrierte Flash-Plug-in einbinden. Firefox- und Opera- sowie Vivaldi-Nutzer müssen sich immer noch getrennt um Flash-Updates kümmern. Bookmarkverwaltung sowie kleine Komfortfeatures wie automatisches Ausfüllen von Webformularen haben alle Browser im Test an Bord. Doch wer an der Optik seines Browser schrauben will, muss zu Chrome, Firefox oder Opera greifen. Die Microsoft-Browser und Vivaldi erlauben nur eingeschränkte Schönheitskorrekturen.

Einige kleine Ausstattungsmängel fielen im Test auf: Vivaldi kann sich als einziger Browser nicht mit anderen Installationen synchronisieren, Firefox bietet unter Windows kein deutsches Wörterbuch für die Rechtschreibkorrektur an und der Internet Explorer unterstützt den WebRTC-Standard für Audio- und Videokonferenzen im Browser nicht. Apropos Standards: Chrome, Firefox und Opera sind top beim Abspielen von typischen Audio- und Videoformaten. Und HTML5, das zunehmend Tools und Plug-ins zur Medienwiedergabe verdrängen wird, ist bei Chrome und Vivaldi am besten umgesetzt sowie mit kleinen Abstrichen auch bei Opera.

Baustelle Sicherheit

Aufholbedarf besteht vor allem bei der Sicherheit, und deshalb gibt es in dieser Disziplin im Test nirgends 100 Punkte. Microsoft verteilt alle vier Wochen Security-Updates, Firefox und Chrome werden alle sechs Wochen aktualisert. Wir haben die Browser mit Security-Benchmarks auf Schwachstellen bei Cross-Site-Scripting oder Address-Spoofing getestet. Dabei erreichten Chrome und die beiden Chromium-basierten Browser Vivaldi und Opera die meisten Punkte. Auto-Updates, Passwortmanager und einen eingebauten Surfschutz haben alle Browser an Bord. Letzterer prüft Webseiten anhand ihrer Reputation und Downloads auf verseuchte Inhalte. Firefox hat mit dem Schutz per Sandboxing noch Probleme und hinkt deshalb der Konkurrenz bei der Sicherheit hinterher. Immerhin ist er neben Chrome der einzige Browser, der per Click-to-Play-Funktion Plug-ins sauber im Zaum halten kann. Überrascht hat uns zudem, dass die aktuelle Vivaldi-Version noch keinen anonymen Privatmodus anbietet. Microsoft Edge sticht mit einer umfangreichen Liste von Browserdaten heraus, die sich leicht löschen lassen. Einen Reset-Knopf für das Zurücksetzen aller Einstellungen auf den Auslieferungszustand gibt es aber nicht – der Internet Explorer hatte den praktischen Button noch.

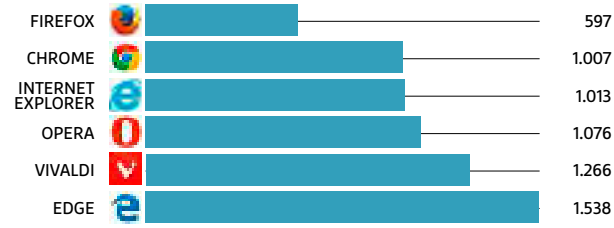
testtechnik@chip.de

AUS DEM TESTLABOR

Firefox spart Ressourcen

Ein unnötig hoher Verbrauch von Arbeitsspeicher kann in der Praxis bremsen. Wir haben den RAM-Verbrauch der Browser im Test mit zehn offenen Tabs beispielhaft gemessen.

RAM-VERBRAUCH (ANGABEN IN MBYTE)



Problematische Erweiterungen

Extensions sind das Salz in der Ausstattungssuppe. Vivaldi kämpft hier noch mit Kompatibilitätsproblemen.

Chrome glänzt beim Flash-Nachfolger

Immer mehr Webseiten wie YouTube setzen auf HTML5. Testsieger Chrome ist auch in dieser Disziplin die Nummer 1.

Ein Stück mehr Privatsphäre

Microsoft Edge bietet in den »Einstellungen« prominent die umfangreiche Option »Browserdaten löschen« an.

CHIP Testurteil

Insgesamt ein Testfeld mit durchweg guten Noten, nur der betagte Internet Explorer fällt ab. Die drei Browser mit Chrome-Unterbau sind vorne, Firefox mit Edge im Mittelfeld.

Testsieger Chrome ist fast überall top. Kein anderer Browser ist so schnell und so sicher – auch bei der Ausstattung liegt er vorne.

Microsoft Edge zeigt bei JavaScript-Benchmarks, dass man Chrome ärgern kann. Aktuell fehlen ihm vor allem Extensions.

Firefox rettet sich mit klasse Bedienung und enormer Ausstattung vor Edge. Bessere Plätze gibt es nur mit besserer Technik.

Opera und Vivaldi sind klasse Alternativen für alle, die Top-Technik, aber keinen Google-Browser haben wollen.

So testet CHIP Browser

Folgendes Testkonzept haben wir für die Browser verwendet:

30 % **Bedienung (30 Prozent)** Bewertet wird die Nutzerführung und Handhabung vom Start weg. Wie gut lassen sich Einstellungen finden? Wie erledigen die Browser Alltagsaufgaben?

30 % **Sicherheit (30 Prozent)** Neben Benchmark-Tests auf klassische Browserlücken beurteilen wir hier auch Schutztechniken wie Sandboxing und Einstellungen zur Plug-in-Sicherheit.

30 % **Speed (30 Prozent)** Hierunter fallen gezielte Messungen der JavaScript-Verarbeitung, 3D-Beschleunigung sowie umfangreiche Speed-Benchmarks mit typischen Webaktionen.

10 % **Ausstattung (10 Prozent)** Wie gut sind die Browser im Auslieferungszustand ausgestattet und wie ist es um die gezielte Erweiterung mit Funktionen bestellt?

Browser im Test

	CHROME	OPERA	VIVALDI	FIREFOX	EDGE	IE
Platz	1	2	3	4	5	6
Gesamt	**95,1**	**90,4**	**88,9**	**87,6**	**82,8**	**71,8**
Bedienung (30 Prozent)	87	85	89	**100**	84	78
Sicherheit (30 Prozent)	97	90	83	83	86	86
Speed (30 Prozent)	**100**	99	97	77	82	53
Ausstattung (10 Prozent)	**100**	82	82	97	73	67
TECHNISCHE DATEN						
Hersteller	Google	Opera	Vivaldi	Mozilla	Microsoft	Microsoft
Getestete Version	44.0.2402.157	31.0	1.0.219.50	40.0.2	201.024.016.384	11.0.9899.0
Betriebssysteme	Windows/ OS X/Linux	Windows/ OS X/Linux	Windows/ OS X/Linux	Windows/ OS X/Linux	Windows 10	Windows
Rendering-Engine	Blink	Blink	Blink	Gecko	EdgeHTML	Trident
JavaScript-Engine	V8	V8	V8	JägerMonkey	Chakra	Chakra
32/64 Bit	■/■	■/□	■/■	■/□	■/■	■/■
Hardware-Beschleunigung	■	■	■	■	■	■
Multiprozess-Architektur	■	■	■	□	■	■
AUSSTATTUNG						
PDF/Flash integriert	■/■	■/□	■/□	■/□	■/□*	□/□**
Erweiterungen	■	■	experimentelle Chrome-Extensions	■	in Planung	nur wenige
Standard-Suchmaschine	Google	Google	Google	Google	Bing	Bing
Synchronisation	über Google-Konto	über Opera-Konto	□	über Firefox-Konto	über MS-Konto	über MS-Konto
Bookmark-Manager	■	■	■	■	■	■
Design anpassbar	■	■	eingeschränkt	■	eingeschränkt	eingeschränkt
Nutzerprofile	■	□	□	■	an Windows-Benutzer gebunden	an Windows-Benutzer gebunden
Rechtschreibprüfung	■	■	■	■***	■	■
Autofill bei Webformularen	■	■	■	■	■	■
WebRTC	■	■	■	■	■	□
H.264/Ogg Theora/WebM/AAC/MP3/Ogg Vorbis	■/■/■/■/■/■	■/■/■/■/■/■	□/■/■/□/□/■	■/■/■/■/■/■	■/□/□/■/■/□	■/□/□/■/■/□
Reset-Funktion	■	□	□	■	□	■
SICHERHEIT						
Auto-Update	■	■	■	■	■	■
Surfschutz	■	■	■	■	■	■
Passwortmanager	■	■	■	■	■	■
Sandbox	■	■	■	eingeschränkt	■	■
Click-to-Play	■	□	□	■	□	□
Privatmodus	■	■	□	■	■	■
MESSWERTE						
Browsermark (Allround-Test)	5.036 Punkte	4.883 Punkte	4.970 Punkte	4.072 Punkte	2.869 Punkte	2.727 Punkte
Octane (JavaScript)	22.789 Punkte	22.424 Punkte	22.213 Punkte	17.791 Punkte	24.074 Punkte	11.991 Punkte
BMark (GPU-Beschleunigung)	1.666 Punkte	1.985 Punkte	1.416 Punkte	737 Punkte	1.092 Punkte	768 Punkte
Browserscope (Security)	16 von 17 Punkten	16 von 17 Punkten	16 von 17 Punkten	14 von 17 Punkten	15 von 17 Punkten	15 von 17 Punkten
HTML5Test (Webstandards)	526 von 555 Punkten	525 von 555 Punkten	526 von 555 Punkten	466 von 555 Punkten	440 von 555 Punkten	348 von 555 Punkten

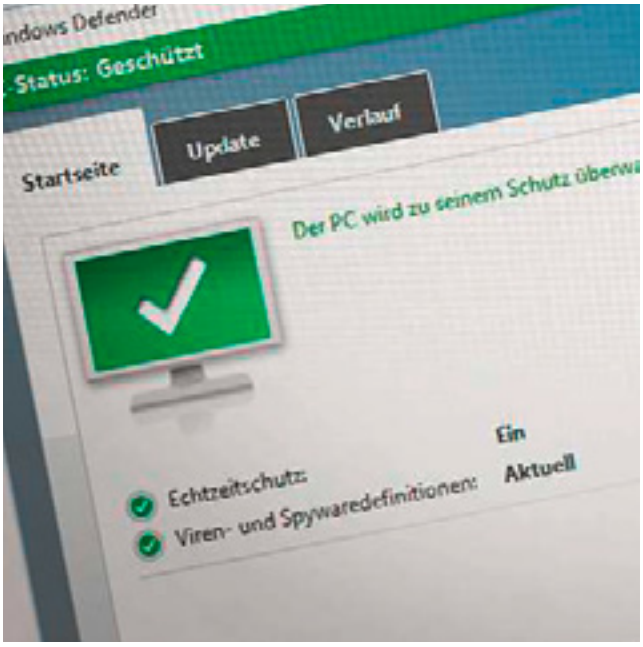
*IN WINDOWS 10 **IN WINDOWS (AB WINDOWS 8)
***UNTER WINDOWS KEIN DEUTSCHES WÖRTERBUCH

SPITZENKLASSE (100–90,0) OBERKLASSE (89,9–75,0) MITTELKLASSE (74,9–45,0) NICHT EMPFEHLENSWERT (44,9–0)
ALLE WERTUNGEN IN PUNKTEN (MAX. 100) | ■ JA □ NEIN

Schutz vor Viren & Co: Defender

Der Windows Defender ist fest ins Betriebssystem integriert und schützt Ihren Rechner vor Viren und Spyware – ganz ohne Ihr Zutun

Von Artur Hoffmann und Angelika Reinhard



Bis zur Veröffentlichung von Windows 7 waren im Microsoft-Betriebssystem überhaupt keine Security-Tools integriert – heute kaum mehr vorstellbar. Seitdem hat Microsoft in Sachen Computersicherheit kräftig nachgebessert. So bringt Windows 10 etwa mit Windows Hello ein Sicherheitsfeature mit, das die Nutzung des Betriebssystems zugleich vereinfachen und sicherer machen soll. Ebenfalls neu ist das Antimalware Scan Interface (AMSI). Diese Schnittstelle soll den Anwender indirekt besser vor Schadsoftware schützen und kann auch von Drittanbietern, etwa Herstellern von Antivirensoftware, genutzt werden.

Mit dem Windows Defender ist – wie bereits bei Windows 8 – ein grundlegender Schutz vor Viren und Spyware an Bord. Der Defender ist fest ins Betriebssystem integriert und ist nach einer Installation von Windows 10 automatisch aktiviert – es sei denn, auf Ihrem Rechner läuft ein Antivirenprogramm eines anderen Anbieters. Da der Defender quasi nur einen Basis-Schutz bietet, belegt er bei Tests von Antivirenprogrammen eher hintere Plätze. Wer einen Premium-Schutz mit vielen Funktionen wünscht, sollte daher auf ein alternatives Produkt wie etwa Bitdefender Internet Security zurückgreifen (Vollversion auf DVD, Workshop auf Seite 96).

Windows SmartScreen anpassen

Die Systemkomponente SmartScreen überwachte bereits unter Windows 7 alle Dateien, die mit dem Internet Explorer geladen wurden. Seit Windows 8 überprüft die Funktion hingegen alle Downloads – unabhängig vom verwendeten Browser. Wird eine Anwendung als unsicher eingestuft, erhalten Sie einen Warnhinweis. Aus Sicherheitsgründen ist der Schutzmechanismus in der Grundeinstellung so konfiguriert, dass vor dem Ausführen einer solchen unsicheren Datei die Genehmigung des Administrators erforderlich ist. Das kann in der täglichen Praxis manchmal lästig sein.

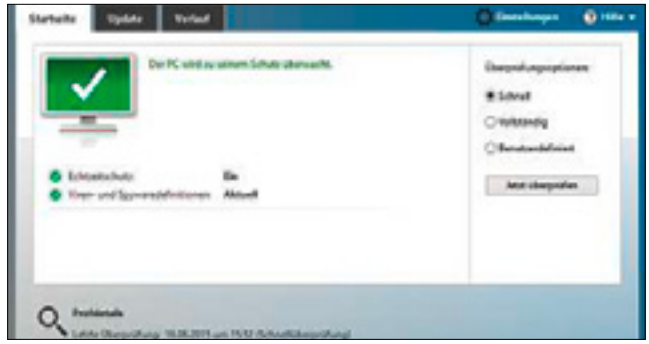
- So passen Sie die Einstellungen des SmartScreen-Filters an: Klicken Sie mit der rechten Maustaste auf den Windows-Startbutton und wählen Sie anschließend »Systemsteuerung | System und Sicherheit | Sicherheit und Wartung«. In der linken Spalte entscheiden Sie sich für »Windows SmartScreen-Einstellungen ändern«.
- Nicht empfehlenswert ist, über die Option »Keine Aktion« den Windows SmartScreen komplett zu deaktivieren. Sind Sie aber häufig ohne Administratorenrechte auf Ihrem Computer unterwegs und möchten sich nicht wegen jeder Warnung von Windows SmartScreen als Admin anmelden, aktivieren Sie das Optionsfeld »Vor dem Ausführen unbekannter Apps warnen, aber keine Administratorgenehmigung erforderlich machen«.

COMPOSING: VERONIKA ZANGL

Den PC schützen mit Windows Defender

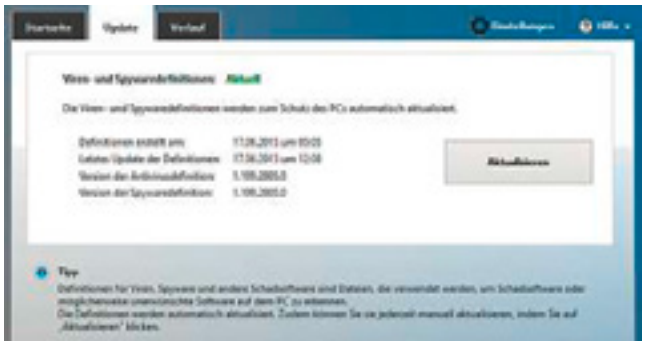
1 Defender aufrufen

Um den Windows-Virenschutz aufzurufen, geben Sie »defender« in die Suchleiste ein und klicken auf »Windows Defender«. Alternativ erreichen Sie den Defender per Doppelklick auf das Mauer-Symbol, das Sie rechts unten in Ihrer Taskleiste finden (ggf. müssen Sie zuvor auf den Pfeil klicken, um alle Symbole anzeigen zu lassen).



2 Standardeinstellungen

Nach einer Neuinstallation von Windows 10 ist der Defender immer aktiviert – es sei denn, Sie haben einen anderen Virenschutz im Einsatz. Der Defender-Startseite entnehmen Sie unter anderem, ob das Schutzprogramm auf dem aktuellen Stand ist und wann die letzte Überprüfung stattgefunden hat.

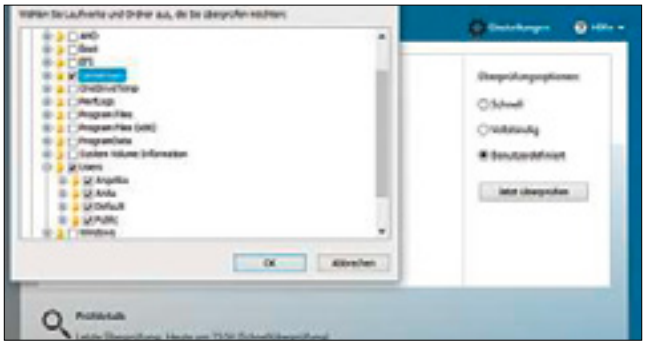


3 Manuelles Update

Die Viren- und Spyware-Definitionen sind nicht auf aktuellem Stand, etwa weil Sie längere Zeit nicht mit dem Internet verbunden waren? In diesem Fall können Sie die Aktualisierung auch manuell anstoßen, indem Sie die Registerkarte »Update« wählen und »Aktualisieren« anklicken.

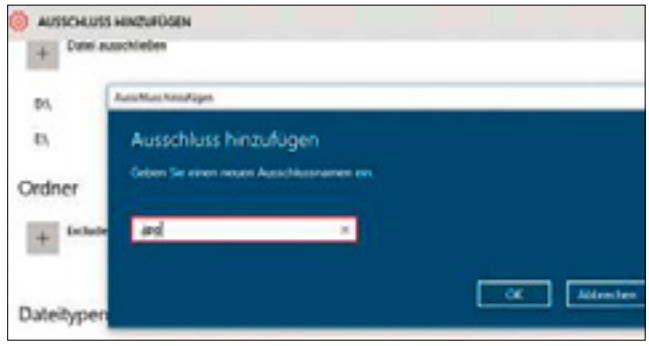
4 Vollständige Überprüfung

Möchten Sie einen vollständigen Systemcheck durchführen? Dann wechseln Sie auf das Register »Startseite«, wählen Sie den Eintrag »Vollständig« und bestätigen Sie mit »Jetzt überprüfen«. Windows Defender scannt daraufhin das gesamte System, was ohne Weiteres eine Stunde und sogar länger dauern kann.



5 Bestimmte Verzeichnisse scannen

Sie möchten nicht Ihr gesamtes System, sondern nur bestimmte, von Ihnen selbst definierte Dateien oder Ordner durchsuchen lassen? Dann führt der Weg über die Option »Benutzerdefiniert«. Nach einem Klick auf »Jetzt überprüfen« wählen Sie manuell die gewünschten Verzeichnisse aus und bestätigen mit »OK«.



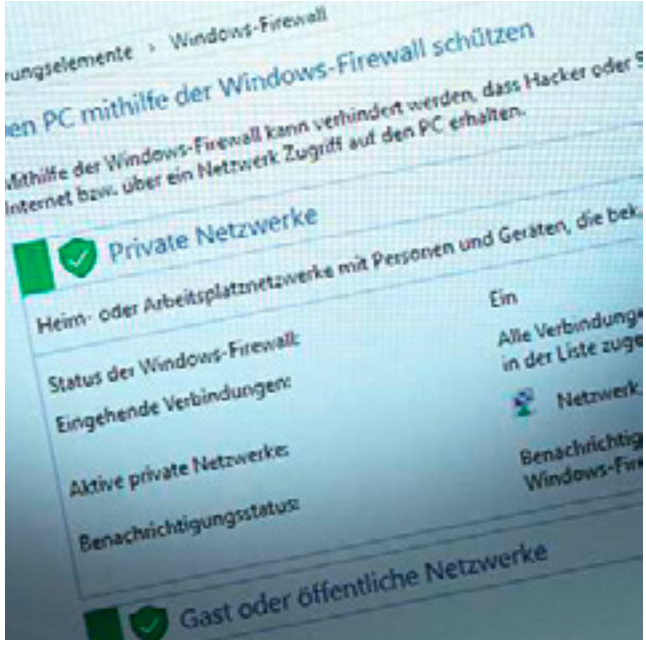
6 An den Stellschrauben drehen

Ein Klick auf »Einstellungen« bringt Sie zur Schaltzentrale des Defenders. Hier lässt sich der Echtzeitschutz deaktivieren – das sollten Sie aber wirklich nur tun, wenn auf Ihrem System ein anderer Virenschutz aktiv ist. Sinnvoller ist die Option »Ausschlüsse«: Hier lassen sich etwa bestimmte Dateitypen vom Scan ausschließen.

Mehr Sicherheit dank Windows Firewall

Mit der ins Betriebssystem integrierten Firewall verhindern Sie Zugriffe von Apps aufs Internet und regeln Empfang und Versand von Datenpaketen

Von Artur Hoffmann und Angelika Reinhard



Die Firewall informiert Sie per Warnhinweis über unbekannte Apps. Die Entscheidung, was nun zu tun ist, liegt bei Ihnen

Wie bereits die Vorgängerversionen verfügt Windows 10 über eine integrierte Firewall – genau gesagt sogar über zwei davon. Auf der einen Seite steht der seit Windows XP bekannte Schutzmechanismus, auf der anderen Seite wacht die als „Windows-Firewall mit erweiterter Sicherheit" bezeichnete Funktion über das System. Der Unterschied: Während die altbekannte Firewall ausschließlich auf den eingehenden Datenverkehr achtet, ist der zweite Schutzmechanismus in der Lage, auch ausgehende Datenpakete zu filtern – gemäß vom Nutzer vorgegebenen Richtlinien. Dies soll verhindern, dass auf dem PC installierte Apps Daten ohne das Wissen des Anwenders übertragen.

Die Windows Firewall unterscheidet zwischen verschiedenen Netzwerktypen, nämlich dem „privaten Netzwerk" und dem „öffentlichen Netzwerk". So haben Sie die Möglichkeit, etwa für das „öffentliche Netzwerk" rigidere Einstellungen zu treffen, bis hin zu »Alle eingehenden Verbindungen blockieren«.

Wenn Sie eine Anwendung starten, die Windows 10 unbekannt ist, macht Sie ein Warnhinweis darauf aufmerksam, dass die Windows-Firewall einige Funktionen dieser Anwendung blockiert hat. Sofern Sie diesem Programm den Internetzugriff gestatten wollen, klicken Sie auf »Zugriff zulassen«. Ist Ihnen die Anwendung jedoch unbekannt, sollten Sie den Zugriffsversuch mit einem Klick auf »Abbrechen« unterbinden. Die Windows-Firewall merkt sich alle von Ihnen getroffenen Entscheidungen, sodass nicht bei jedem Programmstart nachgefragt wird. Sie können die Liste der zugelassenen Apps jedoch selbst anpassen (siehe Schritt 3 rechts).

Noch sehr viel genaueres Feintuning erlaubt die „Windows Firewall für erweiterte Sicherheit". Über die in der linken Randspalte untergebrachten Funktionen »Eingehende Regeln« und »Ausgehende Regeln« können Sie konkrete Firewall-Regeln definieren. Standardmäßig wird mit Ausnahme des Kern-Netzwerkverkehrs der gesamte unaufgefordert eingehende Datenverkehr blockiert. Sie müssen also benutzerdefinierte Regeln erstellen, damit andere Datenpakete durch die Firewall gelassen werden. Auch wird in der Grundeinstellung der gesamte ausgehende Datenverkehr zugelassen. Sie müssen Apps und Funktionen also explizit verbieten, Daten zu versenden. Ein Schritt-für-Schritt-Assistent hilft dabei.

Hinweis: Auf der DVD befindet sich die Vollversion Bitdefender Internet Security mit Virenschutz und Firewall (Workshop auf Seite 96). Falls Sie diese Software oder eine andere Security-Lösung mit Firewall verwenden, wird die Windows-eigene Firewall deaktiviert.

COMPOSING: VERONIKA ZANGL

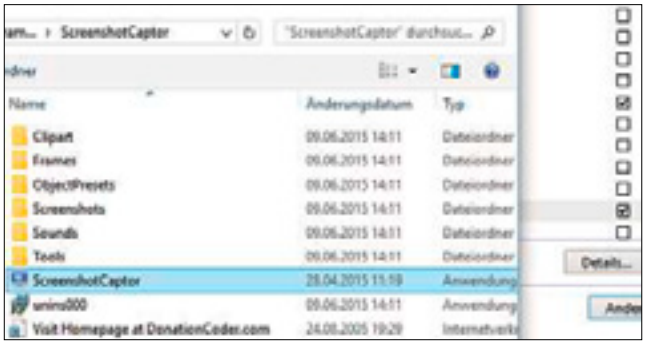
Feintuning der Windows Firewall

1 Firewall aufrufen

Um zu den Einstellungen der Windows Firewall zu gelangen, wählen Sie nach einem rechten Mausklick auf den Windows-Startbutton »Systemsteuerung | System und Sicherheit | Windows Firewall«. Um Anpassungen an den Firewall-Einstellungen durchzuführen, müssen Sie über Administratorrechte verfügen.

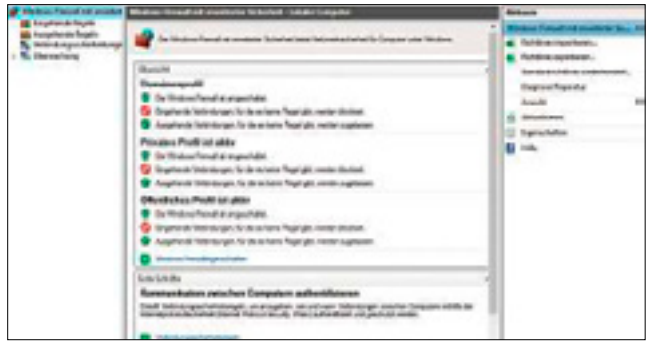
2 Netzwerktypen anpassen

Wählen Sie links »Windows-Firewall ein- oder ausschalten«, um die Einstellungen für die einzelnen Netzwerktypen einzusehen und anzupassen. Wenn Sie nicht immer informiert werden möchten, dass die Windows-Firewall den Internetzugriff einer App geblockt hat, deaktivieren Sie die Option »Benachrichtigen, wenn ...«.



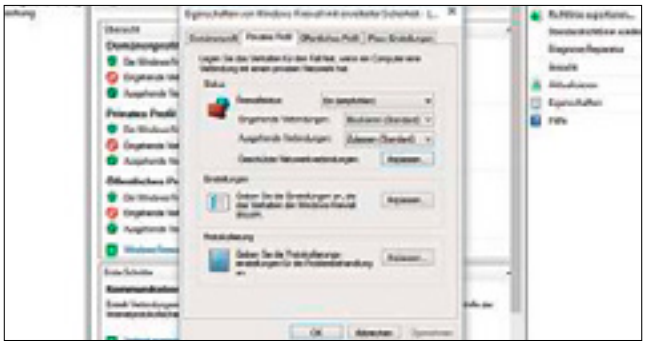
3 Liste zugelassener Apps bearbeiten

Wie bereits erwähnt, „merkt“ sich Windows, welche Anwendungen Sie zulassen möchten. Diese Liste können Sie jedoch auch selbst bearbeiten. Wählen Sie »Eine App oder ein Feature ... zulassen«, klicken Sie im nächsten Fenster auf »Andere App zulassen« und durchsuchen Sie dann Ihren Rechner nach der gewünschten App.



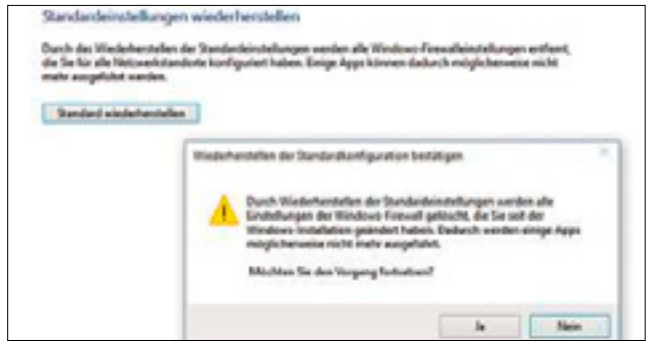
4 Feintuning für versierte Anwender

Ein Klick auf »Erweiterte Einstellungen« führt Sie zu den Profi-Einstellungen der Firewall. Über die Funktionen »Eingehende Regeln« und »Ausgehende Regeln« können Sie nämlich konkrete Firewall-Regeln definieren, um etwa Datenpakete, die eigentlich geblockt würden, dennoch durch die Firewall zu schleusen.



5 Netzwerkverbindungen zulassen

Wählen Sie (nach wie vor im Dialog „... erweiterte Sicherheit“) rechts die »Eigenschaften«. Möchten Sie eine der vorhandenen Netzwerkverbindungen – etwa über Bluetooth – von der Überwachung ausnehmen, klicken Sie bei »Geschützte Netzwerkverbindungen« auf »Anpassen« und entfernen das entsprechende Häkchen.



6 Zurück auf Anfang

Sie haben etwas den Überblick verloren, welche Regeln Sie definiert, welche Apps zugelassen oder welche Verbindungen Sie genehmigt haben? Auch kein Problem: Ein Klick auf »Standard wiederherstellen« links im Hauptfenster stellt den Ausgangszustand wieder her. Alle Ihre individuellen Einstellungen sind dann aber weg.

Nie wieder Datenverlust

Windows 10 bietet ein paar wichtige Tools und Funktionen, um Ihre Daten zu sichern. Wir zeigen, wie Sie diese optimal einsetzen

Von Thorsten Franke-Haverkamp

Datensicherung mit Windows 10

Das neue Windows bietet einige Möglichkeiten, um sich vor Datenverlust zu schützen. Wir zeigen, wie es geht.

- ►Dank des Dateiversionsverlaufs können Sie immer zu einem früheren Zustand einer Datei zurückkehren.
- ►Mit einem Systemabbild sichern Sie ein ganzes Laufwerk.

Sie kennen vielleicht das Bonmot: „Es gibt prinzipiell zwei Arten von Computernutzern – solche, die bereits regelmäßige Backups anlegen, und diejenigen, die es noch nicht tun (und noch auf den ersten Datencrash warten)“. Lassen Sie es nicht so weit kommen, dass erst ein Datenverlust eintreten muss. Mit dem neuen Windows 10 haben Sie nämlich bereits einige hilfreiche Funktionen und Programme an der Hand, mit denen Sie nicht nur Ihre Dateien, sondern auf Wunsch auch Ihr gesamtes System sichern können.

Eines müssen wir jedoch vorwegschicken: Eine individuell abgestimmte Backup-Strategie mit entsprechender Software und Sicherung auf einem externen (Netz-)Laufwerk ersetzt Windows nicht. Dies alles ist vielmehr als Ergänzung zu verstehen. Eine kurze Anleitung, wie Sie zusätzlich automatisierte, individuelle Backups anlegen, finden Sie auf der übernächsten Seite.

Wichtig: Musik, Fotos, Dokumente

So ärgerlich es auch wäre, wenn etwa Windows 10 komplett neu installiert werden müsste, es wäre dennoch kein Vergleich zu einem richtigen Datenverlust. Fotos oder eigene Videos etwa sind unwiederbringlich dahin. Das Gleiche gilt für viele andere Dokumente. Diese persönlichen Dateien stehen also bei einer Datensicherung an oberster Stelle. Deshalb hat Microsoft sie auch in sogenannten Bibliotheken zusammengefasst. Sie finden diese Daten übrigens in der Verzeichnisstruktur von Windows 10 über den Explorer unter »Lokaler Datenträger | Benutzer | Ihr Benutzername«, also beispielsweise unter der Adresse »C:\User\Name«.

Eine praktische Möglichkeit, diese Daten automatisch online zu sichern, ist OneDrive, die kostenlose Cloud für alle Windows-Nutzer. Wie man diese einrichtet, haben wir im Artikel auf Seite 58 beschrieben. Daher empfehlen wir die Aktivierung von OneDrive mit jeder Windows-10-Installation. Allerdings setzt dieser Dienst eine schnelle Internetanbindung voraus, da in der Regel nur dann auch genügend Bandbreite für das Hochladen etwa der eigenen Bilder und Filme zur Verfügung steht und dieser Upload sonst Stunden in Anspruch nehmen könnte. Außerdem ist der kostenlose Speicherplatz auf 15 GByte beschränkt. Somit eignet sich dieser nicht für umfangreichere Archive. Es sei denn, man mietet zusätzlichen Speicherplatz kostenpflichtig dazu.

Für größere Datenmengen eignet sich daher eher eine lokale Sicherung. Sie ist ohnehin zusätzlich zum Online-Speicher zu empfehlen. Windows 10 bietet hier mit dem Dateiversionsverlauf eine

COMPOSING: VERONIKA ZANGL

Clevere Sicherung mit Versionsverwaltung

1 Vorbereitungen

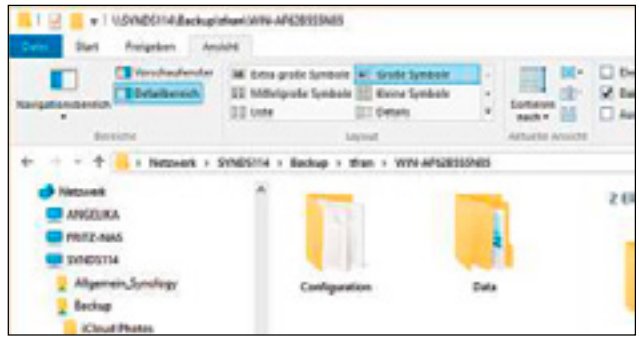
Der Dateiversionsverlauf ist eine äußerst nützliche, permanente Sicherungsmethode in Windows 10, und jeder sollte sie zumindest einmal ausprobieren. Allerdings benötigen Sie ein separates Laufwerk für Ihre Sicherung. Dies kann zum Beispiel eine zweite interne Harddisk, eine USB- oder eine Netzwerkfestplatte (NAS) sein.

2 Dateiversionsverlauf einschalten

Klicken Sie in den »Einstellungen« auf »Update und Sicherheit« und »Sicherung«. Per »Laufwerk hinzufügen« wählen Sie Ihr Ziellaufwerk aus. Dies können Sie anschließend über »Weitere Optionen« nach Belieben ändern. Klicken Sie auf »Einschalten« und warten Sie die erste Sicherung ab.

3 NAS als Sicherungslaufwerk

Noch besser als eine externe Festplatte ist eine Netzwerkfestplatte (NAS). Klicken Sie auf »Laufwerk hinzufügen | Alle Netzwerkadressen anzeigen« und wählen Sie Ihre NAS sowie Ihr Backup-Verzeichnis aus. Bestätigen Sie nun mit »OK« und klicken Sie zum Abschluss auf »Einschalten«.



4 Sicherungsdateien

Die erste Sicherung kann – je nach Datenmenge – über eine Stunde dauern. Standardmäßig werden alle persönlichen Einstellungen, Musik, Fotos, Videos und Dokumente gesichert. Sie finden die Sicherungen im Ziellaufwerk unter Ihrem Benutzer- und Rechnernamen aufgeteilt in den Ordnern »\Configuration« und »\Data«.

5 Sicherungseinstellungen ändern

Sie entscheiden selbst, wann und was mit dem Dateiversionsverlauf gesichert werden soll. Alle Optionen finden Sie unter »Einstellungen | Update und Sicherheit | Sicherung | Weitere Optionen«. Hier können Sie etwa neue Ordner in die Sicherung mit aufnehmen oder Ordner von der Sicherung ausschließen.

6 Dateien wiederherstellen

Öffnen Sie »Einstellungen | Sicherung | Weitere Optionen | Dateien von einer aktuellen Sicherung wiederherstellen«. Über den grünen Knopf können Sie Dateien wiederherstellen; über die Rechts-/Links-Schaltflächen wechseln Sie zwischen verschiedenen Versionen. Die Vorschaufunktion (Doppelklick) hilft bei der Auswahl.

äußerst praktische und leicht zu bedienende Funktion an. Alles, was Sie benötigen, ist eine zweite interne oder externe Festplatte oder ein Netzwerkspeicher (NAS). Mit dem Dateiversionsverlauf werden nicht nur alle persönlichen Dateien wie Musik, Fotos und Dokumente automatisch permanent gespeichert, sondern Sie können auch zwischen verschiedenen Versionen einer Datei hin und her wechseln. Falls Sie sich also beispielsweise bei der Bildbearbeitung eines Fotos vertan haben, stellen Sie so leicht wieder den Originalzustand her. Wie der Dateiversionsverlauf funktioniert, zeigen wir in unserem Workshop auf Seite 91.

Weitere Systemtools und ihre Grenzen

Obwohl beides bei Windows 10 unter der Rubrik »System und Sicherheit« steht, verfolgt doch die Funktion »Sichern und Wiederherstellen« einen ganz anderen Ansatz als der Dateiversionsverlauf. Hierbei geht es nämlich darum, ein Abbild (Image) eines kompletten Laufwerks zu erstellen, also inklusive Betriebssystem, Anwendungen und Daten. Wie das funktioniert, erklären wir im Workshop auf der rechten Seite.

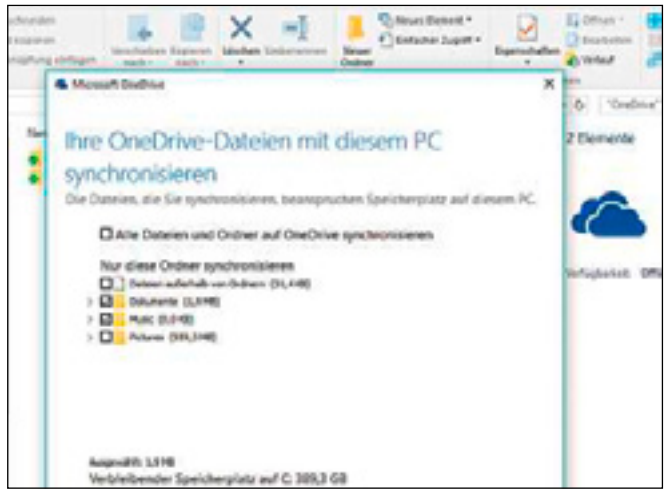
Vollautomatisch geht das Ganze sogar über die Systemwiederherstellung. Sie wird einmal aktiviert und legt dann bei jeder Änderung am System automatisch Wiederherstellungspunkte an (siehe Schritt 6 auf der rechten Seite). Auch hier benötigen Sie, wie auch für das Erstellen von Systemabbildern, einen separaten Datenträger. Auf diese Wiederherstellungspunkte lässt sich Windows immer wieder zurücksetzen, ohne dass dabei die persönlichen Dateien mit verändert werden würden.

Da Windows-Installationen mit der Zeit sehr groß werden können, ist ein komplettes Image nicht immer das Mittel der Wahl. Der größte Nachteil ist aber, dass sich keine einzelnen Dateien extrahieren lassen. Die Wiederherstellungspunkte sichern zudem nur das System und schützen beispielsweise nicht vor versehentlichem Löschen der eigenen Dateien. Wer sich hierbei nicht ausschließlich auf den Dateisystemverlauf verlassen möchte, benötigt also eine weitere, individuelle Backup-Lösung.

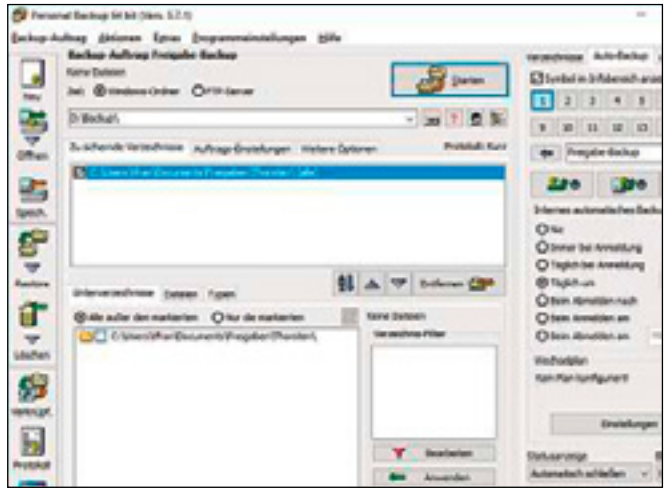
Backup mit System

Professionelle Backup-Tools bieten zahlreiche Optionen. Eine der wichtigsten ist sicherlich ein inkrementelles Backup. Dabei werden nur die Dateien gesichert, die geändert wurden. Man muss also nicht immer sein komplettes Fotoalbum sichern, sondern lässt automatisch im Hintergrund nur alle neuen oder bearbeiteten Fotos auf einen externen Speicher übertragen. Empfehlenswerte kommerzielle Backup-Lösungen sind etwa NovaBackup 17 (ab ca. 40 Euro, **www.novastor.de**) und Langmeier Backup 9 (ca. 50 Euro, **www.langmeier-software.com**). Diese Programme bieten viele Sicherungsoptionen, sind aber gleichzeitig relativ einfach zu bedienen und für Privatanwender erschwinglich.

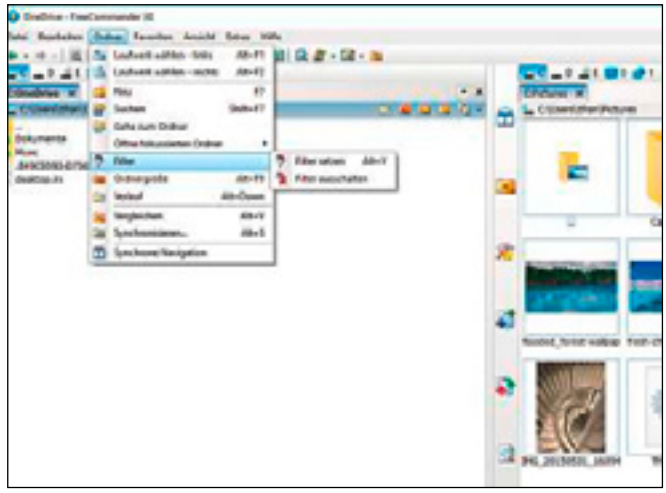
Völlig kostenlos hingegen ist das Programm „Personal Backup“ (auf CHIP). Mit ihm lassen sich zeitgesteuerte Backup-Aufträge anlegen und exakt den persönlichen Wünschen anpassen. Die Oberfläche ist zwar ganz und gar nicht der Windows-10-Optik angepasst, dafür findet man sich relativ schnell mit den vielen Optionen zurecht. Wer hingegen seine Datensicherung lieber manuell durchführen möchte oder wem es vor allem darauf ankommt, Ordner zu synchronisieren, dem sei der ebenfalls kostenlose Free Commander XE empfohlen (auf CHIP). Er schlägt den Windows Explorer beim Kopieren von Daten um Längen.



OneDrive: Sofern die Datenmengen noch überschaubar sind, ist dieser Dienst eine gute Sicherungsoption

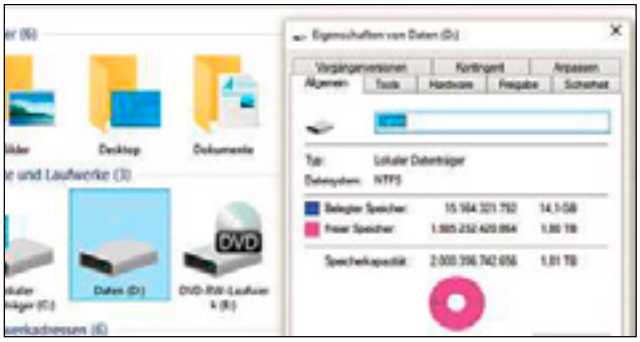


Personal Backup: Auf den ersten Blick etwas unübersichtlich, dennoch eine gute, kostenlose Backup-Lösung



Free Commander XE: Eine exzellente Alternative zum Windows Explorer mit vielen Optionen zur Datensicherung

Sichern des kompletten Systems mit allen Daten

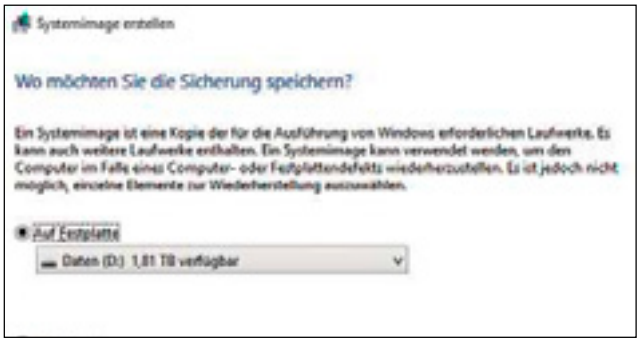


1 Speicherplatz vorbereiten

So praktisch der Dateiversionsverlauf ist, er ersetzt dennoch keine vollständige Systemsicherung. Darum müssen Sie sich also selbst kümmern. Schließen Sie dafür eine zweite interne Harddisk oder eine USB-Festplatte mit ausreichend Speicherplatz an (eine NAS funktioniert natürlich auch).

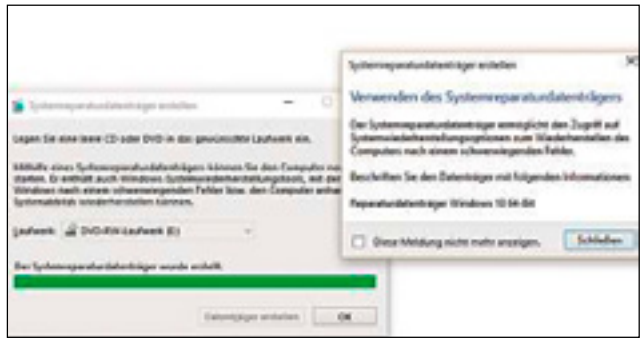
2 Sichern und Wiederherstellen

Windows 10 hat ein recht praktisches Überbleibsel von Windows 7 übernommen: die Möglichkeit, ein komplettes Systemabbild (Image) zu erstellen, also eine exakte Kopie eines Laufwerks. Sie erreichen diese Funktion über »Systemsteuerung | Sichern und Wiederherstellen«. Klicken Sie auf »Systemabbild erstellen«.



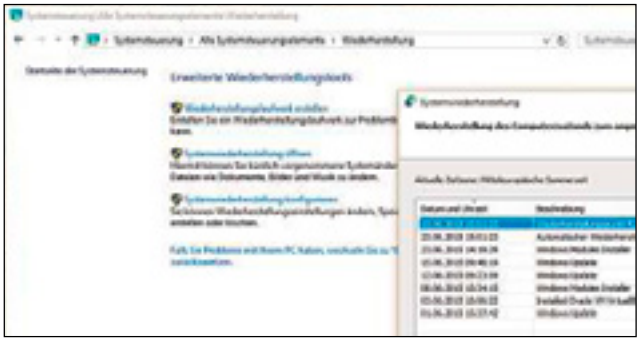
3 Systemabbild erstellen

Wählen Sie Ihr Ziellaufwerk aus und klicken Sie auf »Weiter«. Anschließend wird Ihnen zusammengefasst noch einmal der Sicherungsort sowie das zu sichernde Laufwerk (in der Regel C:) angezeigt. Mit »Sicherung starten« schreiben Sie das Systemabbild. Dies kann je nach Datenmenge einige Zeit dauern.



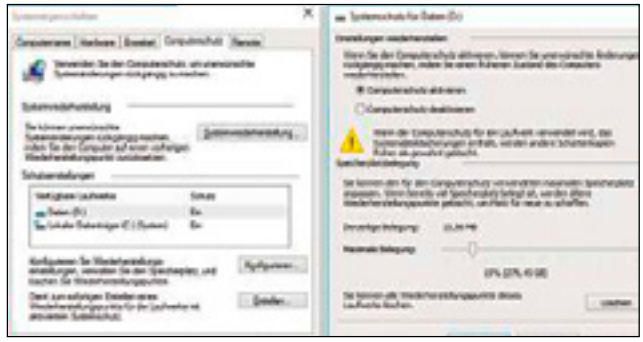
4 DVD für Systemreparatur

Ist die Sicherung erstellt, werden Sie gefragt, ob Sie zusätzlich einen Systemreparaturdatenträger erstellen möchten. Falls Sie einen DVD-Brenner besitzen, können Sie dies bejahen, einen DVD-Rohling einlegen und per Klick auf »Datenträger erstellen« ein solches startfähiges Rettungsmedium anlegen.



5 Abbild wiederherstellen

Um das Abbild wiederherzustellen, geben Sie unten ins Windows-Suchfeld »Wiederherstellung« ein und klicken auf »Systemwiederherstellung öffnen«. Markieren Sie »Weitere Wiederherstellungspunkte anzeigen« und wählen Sie Ihr Systemabbild aus. Mit »Weiter« und »Fertig stellen« starten Sie den Vorgang.



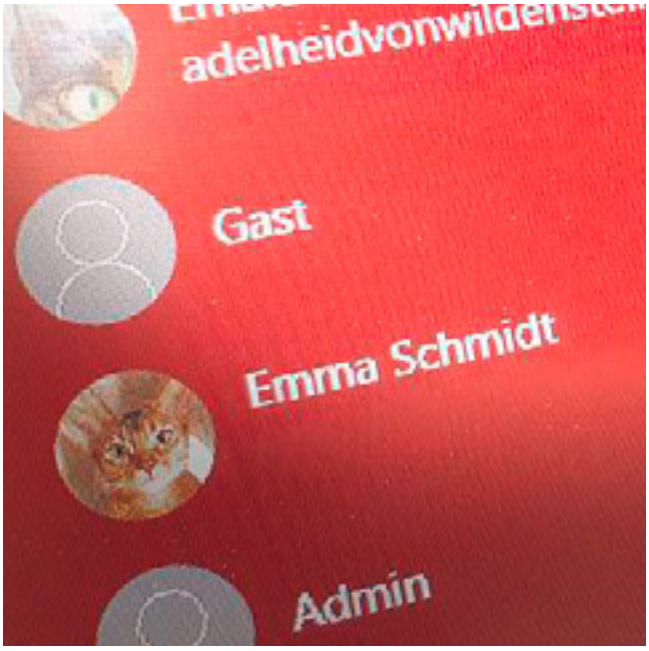
6 Automatische Sicherung

Die Systemwiederherstellung erstellt auf Wunsch automatisch Sicherungspunkte, um den Computer in einen früheren Zustand zu versetzen. Geben Sie ins Windows-Suchfeld »Systemschutz« ein und drücken Sie die Eingabetaste. Klicken Sie auf »Konfigurieren« und markieren Sie »Computerschutz aktivieren«.

Benutzerkonten:
Mehrere Nutzer – ein PC

Hier zeigen wir Ihnen, wie Sie neue Konten anlegen und die Zugriffsrechte Ihrer Kinder mit einem besonderen Konto beschränken können

Von Julia Schmidt



Der wichtigste Unterschied zwischen Benutzerkonten in Windows 10 und Konten in älteren Versionen wie 7, Vista oder XP sind die sogenannten Microsoft-Konten, die mit einer spezifischen E-Mail-Adresse verknüpft sind. Windows-8- und Skype-Nutzern ist das Prinzip zwar schon ein Begriff, aber die Einbettung solcher Konten in Windows 10 ist noch umfassender. Sie werden über kurz oder lang nicht umhinkommen, ein derartiges Konto anzulegen. Denn Sie benötigen eines für sämtliche Microsoft-Services, die in irgendeiner Form geräteübergreifend nutzbar sind, und spätestens, wenn Sie etwas aus dem Windows Store herunterladen möchten.

Übrigens: Wenn Sie Office 365, OneDrive oder andere Web-Apps von Microsoft nutzen oder eine alte Hotmail- beziehungsweise eine Outlook-E-Mail-Adresse besitzen, haben Sie bereits ein Konto.

Unterschiedliche Benutzerkonten sind sehr nützlich, wenn sich mehrere Anwender einen PC teilen. So erhält kein Nutzer Zugriff auf die persönlichen Daten eines anderen. Aus Sicherheitsgründen sollten Sie auch immer ein separates Administrator-Konto einrichten, in das Sie sich nur einloggen, wenn Sie es wirklich benötigen. Für den täglichen Bedarf verwenden Sie ein lokales oder ein Microsoft-Konto, das nicht über Admin-Rechte verfügt.

Jugendschutz in Windows 10: Family Safety

Wie seine Vorgänger bietet auch Windows 10 die Option, die PC-Nutzung von Kindern einzuschränken. Mit dem Service Family Safety können Sie sich unter **https://account.microsoft.com/family** etwa Aktivitätsberichte zum Account Ihres Kindes per E-Mail zuschicken lassen und vieles mehr:

- Legen Sie zuerst ein Kinder-Konto an: Öffnen Sie die Einstellungen, wählen Sie »Konten | Familie und weitere Benutzer| Familienmitglied hinzufügen | Kind hinzufügen«.
- Geben Sie die E-Mail-Adresse des Kindes ein und klicken Sie auf »Weiter«. Es wird nun eine Einladung per E-Mail versendet.
- Bestätigen Sie die Einladung per Klick auf den Link in der E-Mail und loggen Sie sich im sich öffnenden Fenster mit dem Kinder-Account ein. Sie werden nun dazu aufgefordert, weitere Informationen wie etwa das Geburtsdatum einzugeben.
- Gegebenenfalls müssen Sie diesen Schritt mehrmals durchführen, bevor die Einladung korrekt angenommen wird.
- Sobald im Reiter »Familie« in der Menüleiste oben alle angemeldeten Mitglieder angezeigt werden, loggen Sie sich auf der Seite **https://account.microsoft.com/family** mit Ihrem eigenen Account ein.
- Unter dem Reiter »Familie« sollten Sie nun den eben angemeldeten Account sehen. Klicken Sie darauf, um weitere Einstellungen für den Kinder-Account vorzunehmen.

COMPOSING: VERONIKA ZANGL

Neue Benutzerkonten anlegen und verwalten

1 Benutzerkontenverwaltung öffnen

Öffnen Sie die Einstellungen über das Startmenü (oder tippen Sie „Einstellungen“ in die Suchleiste). Wählen Sie im Menü »Konten«. Es wird Ihnen zunächst eine Zusammenfassung des derzeit verwendeten Benutzerkontos angezeigt. Um weitere Konten hinzuzufügen, wählen Sie links im Menü »Familie und weitere Benutzer«.

2 Neues lokales Konto anlegen

Um ein Benutzerkonto anzulegen, wählen Sie »Diesem PC eine andere Person hinzufügen« und im nächsten Fenster zum Beispiel »Ohne Microsoft-Konto anmelden | Lokales Konto«. Vergeben Sie einen Namen, ein Kennwort ist optional. Achtung: Für die Anmeldung eines Microsoft-Kontos benötigen Sie eine Internetverbindung.

3 Andere Konto hinzufügen

Statt eines lokalen Kontos können Sie oben auch eine beliebige E-Mail-Adresse eintragen. Gegebenenfalls werden Sie gleich dazu aufgerufen, ein Microsoft-Konto zu erstellen. Alternativ dazu wird der neue Nutzer durch die weiteren Anmeldeschritte geleitet, sobald er sich das erste Mal anmeldet.

4 Familienmitglieder hinzufügen

Eine besondere Option ist »Familienmitglied hinzufügen«. Alle hinzugefügten Personen müssen per E-Mail angemeldet werden, auch Kinder. Die Einstellungen für die Accounts können Sie dann unter **https://account.microsoft.com/family** anpassen und beispielsweise den Zugriff beschränken und Zeitlimits festlegen.

5 Administratorrechte zuweisen

Das erste Konto, mit dem Sie sich bei der Einrichtung von Windows 10 anmelden, erhält Administrationsrechte. Über die »Systemsteuerung« (Anzeige: »Kleine Symbole«) und »Benutzerkonten | Anderes Konto verwalten« können Sie anderen Konten Rechte einräumen. Wählen Sie ein Konto und dann »Kontotyp ändern«.

6 Benutzerkontensteuerung anpassen

Vorsichtshalber sollten Sie dem bisherigen Admin erst dann die Rechte entziehen, wenn ein anderes Konto Admin-Rechte hat. Als Admin können Sie auch die Benutzerkontensteuerung unter »Systemsteuerung | Benutzerkonten« anpassen. Wählen Sie dazu »Einstellungen der Benutzerkontensteuerung ändern«.

Windows 10 ohne Datenspionage

Das neue Microsoft-System ist fast durchweg geglückt. Doch kein Windows vorher war so scharf auf Ihre Daten. Wir zeigen, wie Sie seine Neugier zähmen

Von Jörg Geiger

Dass Microsoft seinen Testern im Windows Insider Programm etwas auf die Finger schaut, ist logisch. Schließlich muss hier die Nutzung genau unter die Lupe genommen werden, um Windows 10 so weit wie möglich zu optimieren. Doch auch die finale Version von Windows 10 interessiert sich sehr für Ihre Daten – wer nicht aufpasst, verrät (zu) viel über sich. Wir zeigen, wie Sie Windows 10 die Datenspionage wieder abgewöhnen.

1 INSTALLATION Wer die Express-Einstellungen wählt, öffnet die Tür zum Ausspähen

Sie kennen die Situation: Sie wollen eine neue Software ganz schnell ausprobieren und klicken sich durch den Installer. Natürlich lesen die meisten Nutzer dabei weder die AGBs, noch justieren sie die Einstellungen nach. Windows 10 lockt beim Installieren mit den Stichworten »Schnell einsteigen«. Wer jetzt auf »Express-Einstellungen verwenden« klickt, hat verloren. Windows 10 genehmigt sich in diesem Fall jede Menge Rechte, um auf Ihre Daten zuzugreifen. Zum Beispiel erlauben Sie, dass alles, was Sie eintippen, an Microsoft gesendet wird. Wer das verhindern will, klickt an dieser Stelle links unten im Fenster auf den Mini-Text »Einstellungen anpassen« und stellt sämtliche Optionen auf den nächsten zwei Seiten auf »Aus«.

2 LOKALES KONTO Statt eines Microsoft-Kontos bietet Win 10 auch lokale Konten

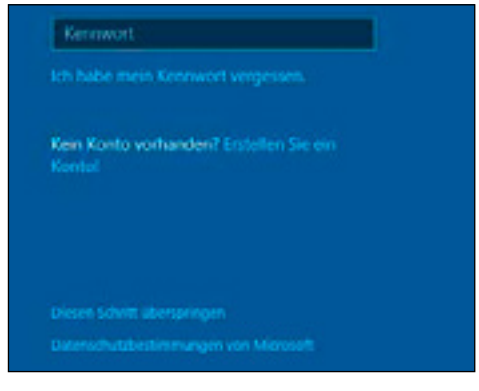
Egal ob Apple, Facebook, Google oder auch Microsoft: Alle großen Firmen aus der Branche möchten ihre Kunden mit eigenen Benutzerkonten binden. Deshalb versucht Windows 10 – wie schon die Vorgänger Windows 8 und 8.1 – die Nutzer bei der Installation zum Login mit einem Microsoft-Konto zu überreden. Und der Nutzer wird regelrecht überrumpelt, denn er sieht erst einmal nur Eingabefelder für Nutzername und Passwort sowie einen Hinweis für Nutzer, die ihr Kennwort vergessen haben. Wer noch kein Microsoft-Konto hat, kann sogar gleich eins anlegen. Ganz unten in kleinerer Schrift ist aber dann die Option versteckt, die Ihnen die Nutzung mit einem lokalen Konto eröffnet. Klicken Sie auf »Diesen Schritt überspringen« und legen Sie auf dem nächsten angezeigten Bildschirm ein ganz normales lokales Konto an. Wenn Sie bereits ein Microsoft-Konto unter Windows 10 haben, können Sie trotzdem ein lokales Konto für die Anmeldung nutzen. Das geht in den Einstellungen unter »Konten«. Klicken Sie bei »Ihr Konto« auf »Stattdessen mit einem lokalen Konto anmelden«.

3 CORTANA Sammelwut an vielen Stellen mit nur einer Einstellung abschalten

Wer mit der Sprachassistentin Cortana experimentiert, holt sich einen neugierigen Begleiter auf den PC. Hier darf man allerdings nicht zu sehr auf Microsoft schimpfen, denn schließlich muss eine Assistentin ihren Herrn gut kennen – sonst kann sie ihm auch nicht unter die Arme greifen. Cortana interessiert sich deshalb natürlich für Ihren Kalender, für Daten aus Programmen, Ihre Eingaben und so weiter.

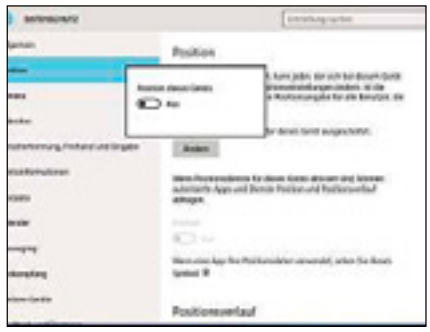
Wer Cortana das abgewöhnen will, klickt neben der Windows-Fahne in das Suchfeld, wählt links in der Leiste das dritte Icon von oben aus und klickt dann auf »Einstel-

1 Vorsicht vor Expresseinstellungen
Im Hinblick auf den Datenschutz ist es nicht ratsam, den Schnelleinstieg zu wählen



2 Lokales Konto
Ein Microsoft-Konto ist zwar praktisch, man braucht es als Nutzer von Windows 10 aber nicht unbedingt

3 Cortana abschalten
Die Sprachassistentin ist sehr neugierig auf Ihre persönlichen Daten. Hier hilft abschalten



4 Standort verbergen
Windows 10 weiß, wo Sie sind. Doch das muss nicht sein, auch wenn manche App das möchte

lungen«. Dann den obersten Schalter auf »Aus« stellen und schon hört Cortana auf mit Datensammeln, denn die Sprachassistentin ist jetzt ausgeschaltet.

4 STANDORT Windows 10 genehmigt sich auch den Zugriff auf Ihren Standort

Auch hier gilt: Manche Dienste brauchen Ihren Standort, um zu funktionieren. Etwa macht ein Kartendienst keinen Sinn, wenn er nicht weiß, wo Sie sind. Ständig und systemweit die eigene Position zu verraten, kann es aber auch nicht sein. Also schalten Sie diese Funktion aus. Das klappt über die »Einstellungen« und den Punkt »Datenschutz«. Klicken Sie auf »Position« und stelllen Sie den Schieberegler auf »Aus«.

5 KAMERA SICHERN App-Zugriff auf eingebaute Kameras justieren

Manche Apps benötigen zwar den Zugriff auf eingebaute Kameras, unter Windows 10 sind die Einstellungen für den Kamerazugriff jedoch sehr großzügig gesetzt. Hier sollten Sie einen Riegel vorschieben. Auch das geht über die »Einstellungen« und den Punkt »Datenschutz«. Klicken Sie auf »Kamera« und legen Sie den Schalter auf »Aus«. Wenn Sie Apps nutzen, die immer Zugriff auf Ihre Kamera haben sollen, können Sie den obigen Schalter auch auf »Ein« stehen lassen und dann unten in der Liste gezielt den Zugriff für einzelne Apps freischalten. So behalten Sie die Kontrolle und verhindern, dass sich Apps unnötig den Kamerazugriff holen.

6 DATENSCHUTZ Weitere Privatsphäre-Einstellungen

Unter »Einstellungen« und dem mittlerweile schon bekannten Menüpunkt »Datenschutz« gibt es noch zahlreiche weitere Einstellungen, mit denen Sie mehr Privatsphäre erreichen. Hier sollten Sie etwa unter dem Punkt »Allgemein« die Verwendung der Werbungs-ID für Apps verbieten.

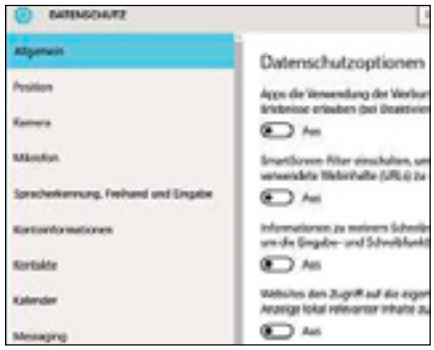
Unter »Mikrofon« schränken Sie die Rechte von Apps ähnlich wie beim Zugriff auf die Kamera ein. Wenn Sie der Meinung sind, keine App muss Sie belauschen, stellen Sie den oberen Schieberegler auf »Aus«. Sollen hingegen nur einzelne Apps das Mikrofon nutzen dürfen, lassen Sie den Schalter oben auf »Ein« und justieren unten in der Liste die einzelnen Anwendungen.

Unter »Kontoinformationen« können Sie Apps den Zugriff auf Namen, Bild und andere Kontoinfos verbieten. Wer Apps komplett zähmen will, entzieht ihnen auch den Zugriff auf »Kontakte«, »Kalender«, »Messaging« und »Funkempfang«. Wichtig: Schauen Sie sich die Liste unter »Hintergrund-Apps« an. Jede App, die nicht ständig laufen muss, sollte auf »Aus« stehen. Unter »Feedback und Diagnose« stellen Sie die »Feedbackhäufigkeit« auf »Nie«.

7 BROWSER Auch Microsofts neuer Browser Edge sammelt fleißig Daten

Microsoft Edge, der Nachfolge-Browser des Internet Explorers, setzt natürlich stark auf Microsofts Suchmaschine Bing und die hauseigene News-Plattform MSN. Diese Dienste tracken das Internet-Verhalten des Nutzers, darunter Suchverlauf und Browser-Historie. Eingaben von URLs werden live an Microsoft übertragen, um proaktiv Websites vorzuschlagen. Und auch Cortana mischt im Browser fleißig mit. Doch das lässt sich alles ändern.

Über das »...«-Menü oben rechts können Sie die »Einstellungen« aufrufen. Dort sollten Sie unter »Neue Tabs öffnen mit« der Punkt »Leere Seite« einstellen. Dann ist hier Schluss mit empfohlenen Inhalten von MSN. Um dies auch der Startseite beizubringen, wählen Sie unter »Öffnen mit« den Eintrag »neuer Tabseite«. Ist Cortana aktiviert, kann der Sprachassistentin die Zusammenarbeit mit Microsoft Edge verboten werden. Das klappt über »Erweiterte Einstellungen anzeigen« und den Punkt »Cortana soll mich bei Microsoft Edge unterstützen«. Stellen Sie den Schieberegler dort auf »Aus«. Auch »Suchvorschläge bei der Eingabe anzeigen« und »Seitenvorhersage verwenden...« schalten Sie dort »Aus«, dann landen Ihre Suchbegriffe nicht mehr automatisch bei Microsoft.



6 Datenschutz tunen
In den Datenschutz-Einstellungen können Sie den Datendurst von Windows 10 einschränken

7 Edge zähmen
Microsoft Edge schickt viele Daten automatisch zu Microsoft. Per Einstellungen zähmen Sie den Browser

Impressum

Chefredakteur	Josef Reitberger (verantwortlich für den redaktionellen Inhalt)
stellv. Chefredakteur	Andreas Hentschel
Art Direction	Stephanie Schönberger
Chefin vom Dienst	Verena Flurschütz
News	Niels Held (Ltg. Print), Markus Schmidt (Ltg. Online); Caren Stella Geiger, Dominik Hayon, Rupert Mattgey, Claudio Müller, Frederik Niemeyer
Test & Technik	Martin Michl (Ltg.); Benjamin Hartlmaier, Fabian von Keudell, Peter Krajewski, Markus Mandau, Christoph Schmidt, Andreas Vogelsang
Multimedia	Andreas Hentschel (Ltg.); Peter Deppner (Lizenzen), Karsten Bunz, Patrick Dörfel
Red. Tablet-Edition	Dominik Hoferer
Testcenter	Wolfgang Pauler (Testchef CHIP); Torsten Neumann (Teamleiter Testcenter), James Curtis, Tomasz Czarnecki, Werner Gaschar, Christoph Giese, Grzegorz Glonek, Stephan Hartmann, Leopold Holzapfel, Martin Jäger, Robert Kraft, Martin Nowakowski, Sven Sebastian, Jacek Wojtowicz
Grafik	Antje Küther (Ltg.); Janine Auer, Esther Göddertz, Doreen Heimann, Isabella Schillert, Andreia Margarida da Silva Granada, Veronika Zangl
Schlussredaktion	Renate Feichter, Birgit Lachmann, Angelika Reinhard
Bildredaktion	Jennifer Heintzschel, Gertraud Janas-Wenger
Bildbearbeitung	Gisela Zach
Assistenz	Verena Flurschütz (Redaktion) Monika Masek (Testcenter)
CHIP Online	Martin Gollwitzer (Chefredakteur CHIP.de), Carl Schneider (Chefredakteur CHIP.de), Lisa Brack (Stellv. Chefredakteurin), Dr. Wiebke Hellmann (Lt. Redakteurin), Florian Holzbauer (Lt. Redakteur), Michael Humpa (Teamleiter Downloads & Apps), Beate Kipphardt (Teamleiterin Software & OS), Michael Ludwig (Ressortleiter), Alexander Schauer (CvD & lt. Schlussredakteur), Kirstin Dedic, Saskia Dittrich, Markus Grimm, Benjamin Heinfling, Andreas Nolde, Matthias Rößler, Dennis Schöberl, Sebastian Schoener, Manuel Schreiber, Christian Schwalb, Rian Voß, Moritz Wanke, Dominik Zientek
	Thomas Mayrhans (Director Product)
Anschrift der Redaktion	St.-Martin-Straße 66, 81541 München Tel. 089 746 42-502 (Redaktion), -253 (Testcenter), -120 (Fax)
Geschäftsführung	Thomas Koelzer (CEO) Markus Scheuermann (COO)
Executive Director	Florian Schuster
Director Distribution	Andreas Laube
Herstellung	Andreas Hummel, Frank Schormüller Medienmanagement Vogel Business Media GmbH & Co. KG 97064 Würzburg
Vertrieb	MZV GmbH & Co. KG 85716 Unterschleißheim Internet: www.mzv.de
Verlag	CHIP Communications GmbH St.-Martin-Straße 66, 81541 München Tel. 089 746 42-0, Fax: 089 746 42-120
	Die Inhaber- und Beteiligungsverhältnisse lauten wie folgt: Alleinige Gesellschafterin ist die CHIP Holding GmbH mit Sitz in der St.-Martin-Straße 66, 81541 München.
Verleger	Prof. Dr. Hubert Burda